ALL INFORMATION SERVICES, INC.

Integrating the World's Technology

AIS Vulnerability Assessment

Report Prepared For:

Customer	Example Customer
Customer Contact	aiscustomer@aisclients.com
Creation Date	7/28/2022
Prepared By	AIS

Summary

Example Customer Overview	
High Risk Vulnerabilities	**102**
Medium Risk Vulnerabilities	**123**
Low Risk Vulnerabilities	**5731**

This assessment's scores are derived from Common Vulnerability and Exposures (CVE) databases which are sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The CVE gets its Common Vulnerability Scoring System (CVSS) rating based on the National Institute of Standards and Technology (NIST) NVD CVSS v2.0 Rating system.

Addressing vulnerabilities is an ongoing process, and the results of this assessment are dynamic. While remediation of items in this report would help to secure your network, a plan must be made to identify and address new vulnerabilities as they are released.

Vulnerability Tests

Quality of Detection (QoD) Type	Tests Performed
Remote Vulnerability	24
Executable Version Unreliable	12
Package	36
Remote Banner Unreliable	19
Executable Version	20
Registry	22
Remote Banner	34
Remote Analysis	21
Remote App	14
Remote Active	22
Exploit	15
General Note	9
Remote Probe	12

High Risk (102)

A High Risk Vulnerability will cause major disruption to a network with additional concern for network/data security. Exploitation of the identified vulnerability will have a significant impact to critical systems of the network. These vulnerabilities might also allow attackers access to critical data.

Risk	**High**		**Threat Type**	Gain a shell remotely		**CVSS**	**10.0**
Summary	The web server was crashed by sending an invalid POST HTTP request with a negative Content-Length field.						
Affected Nodes	192.168.50.58 -						
Impact	An attacker may exploit this flaw to disable the service or even execute arbitrary code on the system.						
Solution	Upgrade your web server.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	HTTP negative Content-Length buffer overflow						

CVE-2015-1635							
Risk	**High**		**Threat Type**	Web Servers		**CVSS**	**10.0**
Summary	This host is missing an important security update according to Microsoft Bulletin MS15-034.						
Affected Nodes	192.168.9.211 -						
Impact	Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.						
Solution	The vendor has released updates. Please see the references for more information.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys Remote Code Execution Vulnerability." MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)						
Detection Method	Send a special crafted HTTP GET request and check the response						
References	https://support.microsoft.com/kb/3042553 https://technet.microsoft.com/library/security/MS15-034 http://pastebin.com/ypURDPc4						

CVE-2019-0708							
Risk	**High**		**Threat Type**	Windows Microsoft Bulletins		**CVSS**	**10.0**
Summary	Microsoft Windows Remote Desktop Services is prone to the remote code execution vulnerability known as BlueKeep.						
Affected Nodes	192.168.11.67 -						
Impact	Successful exploitation would allow an attacker to execute arbitrary code on the target system. An attacker could then install programs, view, change, or delete data, or create new accounts with full user rights.						
Solution	The vendor has released updates. Please see the references for more information. As a workaround enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2. NOTE: After enabling NLA affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.	**Solution Type**	VendorFix				
Additional Details							
CVE Description	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'. Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)						
Detection Method	Sends a specially crafted request to the target systems Remote Desktop Service via RDP and checks the response.						
Findings	By sending a crafted request the RDP service answered with a MCS Disconnect Provider Ultimatum PDU - 2.2.2.3 response which indicates that a RCE attack can be executed.						
References	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708 https://support.microsoft.com/help/4499164 https://support.microsoft.com/help/4499175 https://support.microsoft.com/help/4499149 https://support.microsoft.com/help/4499180 https://support.microsoft.com/help/4500331 https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/ https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.securityfocus.com/bid/108273 http://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Desktop-BlueKeep-Denial-Of-Service.html https://www.malwaretech.com/2019/05/analysis-of-cve-2019-0708-bluekeep.html https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708						

CVE-2001-0249							
Risk	High		**Threat Type**	FTP		**CVSS**	10.0
Summary	The FTPD glob vulnerability manifests itself in handling of the glob command. The problem is not a typical buffer overflow or format string vulnerability but a combination of two bugs an implementation of the glob command that does not properly return an error condition when interpreting the string and then frees memory which may contain user supplied data. This vulnerability is potentially exploitable by any user who is able to log in to a vulnerable server including users with anonymous access. If successful an attacker may be able to execute arbitrary code with the privileges of FTPD typically root.						
Affected Nodes	192.168.11.64 -						
Solution	Contact your vendor for a fix.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Heap overflow in FTP daemon in Solaris 8 allows remote attackers to execute arbitrary commands by creating a long pathname and calling the LIST command, which uses glob to generate long strings. FTPD glob Heap Corruption						
Detection Method							
Findings	You seem to be running an FTP server which is vulnerable to the glob heap corruption flaw which is known to be exploitable remotely against this server. An attacker may use this flaw to execute arbitrary commands on this host.						

Risk	High		**Threat Type**	Malware		**CVSS**	10.0
Summary	An unknown service runs on this port. It is sometimes opened by Trojan horses. Unless you know for sure what is behind it youd better check your system.						
Affected Nodes	192.168.3.103 -						
Solution	If a trojan horse is running, run a good antivirus scanner.					**Solution Type**	Mitigation
Additional Details							
CVE Description	Trojan horses						
Findings	An unknown service runs on this port. It is sometimes opened by thisthese Trojan horses- The Prayer- Lateda.C- Beasty.I						

Risk	High		Threat Type	CISCO		CVSS	10.0
Summary	Several researchers have reported on the use of Smart Install SMI protocol messages toward Smart Install clients also known as integrated branch clients IBC allowing an unauthenticated remote attacker to change the startup-config file and force a reload of the device load a new IOS image on the device and execute high-privilege CLI commands on switches running Cisco IOS and IOS XE Software. Cisco does not consider this a vulnerability in Cisco IOS IOS XE or the Smart Install feature itself but a misuse of the Smart Install protocol which does not require authentication by design. Customers who are seeking more than zero-touch deployment should consider deploying the Cisco Network Plug and Play solution instead.						
Affected Nodes	192.168.4.1 -						
Solution	Cisco has updated the Smart Install Configuration Guide to include security best practices regarding the deployment of the Cisco Smart Install feature within customer infrastructures.				Solution Type		Workaround
Additional Details							
CVE Description	Cisco Smart Install Protocol Misuse						
Findings	The Cisco Smart Install Protocol was detected on the target host.						
References	https://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20170214-smi http://www.securityfocus.com/archive/1/540130 https://2016.zeronights.ru/wp-content/uploads/2016/12/CiscoSmartInstall.v3.pdf http://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/concepts.html#23355						

CVE-2016-8735							
Risk	High		Threat Type	Web Servers		CVSS	10.0
Summary	Apache Tomcat is prone to a remote code execution RCE vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to execute arbitrary code.						
Solution	Update to version 6.0.48, 7.0.73, 8.0.39, 8.5.8, 9.0.0.M13 or later.				Solution Type	VendorFix	
Additional Details							
CVE Description	Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types. Apache Tomcat RCE Vulnerability (Nov 2016)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.48Installationpath port 8080tcp						
References	http://seclists.org/oss-sec/2016/q4/502 https://tomcat.apache.org/security-9.html https://tomcat.apache.org/security-8.html https://tomcat.apache.org/security-7.html https://tomcat.apache.org/security-6.html						

Risk	**High**		**Threat Type**	Web Servers		**CVSS**	**10.0**
Summary	The Apache Tomcat version on the remote host has reached the End of Life EOL and should not be used anymore.						
Affected Nodes	192.168.11.86 -						
Impact	An EOL version of Apache Tomcat is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.						
Solution	Update the Apache Tomcat version on the remote host to a still supported version.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Apache Tomcat End of Life (EOL) Detection (Windows)						
Detection Method	Checks if an EOL version is present on the target host.						
Findings	The Apache Tomcat version on the remote host has reached the end of life.CPE cpeaapachetomcat6.0.24Installed version 6.0.24LocationURL 8080tcpEOL version 6.0EOL date 2016-12-31						
References	https://tomcat.apache.org/tomcat-80-eol.html https://tomcat.apache.org/tomcat-60-eol.html https://tomcat.apache.org/tomcat-55-eol.html https://en.wikipedia.org/wiki/Apache_Tomcat#Releases https://tomcat.apache.org/whichversion.html						

CVE-2000-0002							
Risk	**High**		**Threat Type**	Buffer overflow		**CVSS**	**10.0**
Summary	Remote web server is vulnerable to the too long URL vulnerability. It might be possible to gain remote access using buffer overflow.						
Affected Nodes	192.168.3.253 -						
Impact							
Solution	Upgrade vulnerable web server to latest version.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Multiple buffer overflows in (a) UltraVNC (aka Ultr@VNC) 1.0.1 and earlier and (b) tabbed_viewer 1.29 (1) allow user-assisted remote attackers to execute arbitrary code via a malicious server that sends a long string to a client that connects on TCP port 5900, which triggers an overflow in Log::ReallyPrint; and (2) allow remote attackers to cause a denial of service (server crash) via a long HTTP GET request to TCP port 5800, which triggers an overflow in VNCLog::ReallyPrint. www too long url						

Risk	High		Threat Type	General		CVSS	10.0
Summary	The Windows 7 Server 2008 Operating System on the remote host has reached the end of life and should not be used anymore. Note Both Operating Systems might be covered by extended security updates ESU so this VT is prone to false positives.						
Affected Nodes	192.168.11.110 -						
Solution	Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.			Solution Type	Mitigation		
Additional Details							
CVE Description	Microsoft Windows 7 / Server 2008 End Of Life Detection						
Findings	The Microsoft Windows 7 Operating System on the remote host has reached the end of life.CPE cpeomicrosoftwindows7-sp1Installed versionbuild or SP sp1EOL date 2020-01-14EOL info httpssupport.microsoft.comen-uswindowswindows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962						
References	https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962 https://support.microsoft.com/en-us/help/4456235/end-of-support-for-windows-server-2008-and-windows-server-2008-r2						

CVE-2001-0554							
Risk	High		Threat Type	Gain a shell remotely		CVSS	10.0
Summary	The Telnet server does not return an expected number of replies when it receives a long sequence of Are You There commands. This probably means it overflows one of its internal buffers and crashes.						
Affected Nodes	192.168.9.117 -						
Impact	It is likely an attacker could abuse this bug to gain control over the remote host's superuser.						
Solution	Comment out the 'telnet' line in /etc/inetd.conf.			Solution Type	Mitigation		
Additional Details							
CVE Description	Buffer overflow in BSD-based telnetd telnet daemon on various operating systems allows remote attackers to execute arbitrary commands via a set of options including AYT (Are You There), which is not properly handled by the telrcv function. TESO in.telnetd buffer overflow						
References	http://www.team-teso.net/advisories/teso-advisory-011.tar.gz						

CVE-2000-1209							
Risk	**High**		**Threat Type**	Default Accounts		**CVSS**	**10.0**
Summary	The remote MS SQL server has the default sa account enabled without any password.						
Affected Nodes	192.168.11.47 -						
Impact	An attacker may use this flaw to execute commands against the remote host, as well as read your database content.						
Solution	Disable this account, or set a password to it. In addition to this, it is suggested you filter incoming tcp traffic to this port. For MSDE (OEM versions without MSQL console) : C:\MSSQL7\BINN\osql -U sa At the Password: prompt press <Enter>. Type the following replacing .password. with the password you wish to assign, in single quotes: EXEC sp_password NULL, .password., .sa. go exit				**Solution Type**		Workaround
Additional Details							
CVE Description	The "sa" account is installed with a default null password on (1) Microsoft SQL Server 2000, (2) SQL Server 7.0, and (3) Data Engine (MSDE) 1.0, including third party packages that use these products such as (4) Tumbleweed Secure Mail (MMS) (5) Compaq Insight Manager, and (6) Visio 2000, which allows remote attackers to gain privileges, as exploited by worms such as Voyager Alpha Force and Spida. Microsoft's SQL Blank Password						
Findings	The SQL Server has a blank password for the sa account.						

Risk	**High**		**Threat Type**	Gain a shell remotely		**CVSS**	**10.0**
Summary	The remote web server seems to be vulnerable to a format string attack on the URI. An attacker might use this flaw to make it crash or even execute arbitrary code on this host.						
Affected Nodes	192.168.11.46 -						
Impact	Successful exploitation will allow remote attackers to execute code, read the stack, or cause a segmentation fault in the running application, causing new behaviors that could compromise the security or the stability of the system.						
Solution	Upgrade your software or contact your vendor and inform him of this vulnerability.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Format string on URI						
Detection Method	Send a crafted request via HTTP GET and check whether the server is vulnerable to format string attack.						
References	https://www.owasp.org/index.php/Format_string_attack						

Risk	**High**		**Threat Type**	Web application abuses		**CVSS**	**10.0**
Summary	The installed version of jQuery on the remote host has reached the End of Life EOL and should not be used anymore.						
Affected Nodes	192.168.6.252 -						
Impact	An EOL version of jQuery is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.						
Solution	Update jQuery on the remote host to a still supported version.					**Solution Type**	VendorFix
Additional Details							
CVE Description	jQuery End of Life (EOL) Detection (Linux)						
Detection Method	Checks if an EOL version is present on the target host.						
Findings	The jQuery version on the remote host has reached the end of life.CPE cpeajqueryjquery1.12.4Installed version 1.12.4LocationURL https192.168.6.252wwwjsEOL version 1EOL date unknown						
References	https://github.com/jquery/jquery.com/pull/163						

Risk	High		**Threat Type**	General		**CVSS**	10.0
Summary	The Operating System OS on the remote host has reached the End of Life EOL and should not be used anymore.						
Affected Nodes	192.168.11.14 -						
Impact	An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.						
Solution	Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.					**Solution Type**	Mitigation
Additional Details							
CVE Description	Operating System (OS) End of Life (EOL) Detection						
Detection Method	Checks if an EOL version of an OS is present on the target host.						
Findings	The VMWare ESX ESXi Operating System on the remote host has reached the end of life.CPE cpeovmwareesxi6.0.0Installed versionbuild or SP 6.0.0EOL version 6.0EOL date 2020-03-12EOL info httpswww.vmware.comcontentdamdigitalmarketingvmwareenpdfsupportproduct-lifecycle-matrix.pdf						

CVE-2016-7406							
Risk	High		**Threat Type**	General		**CVSS**	10.0
Summary	Dropbear SSH is prone to multiple vulnerabilities.						
Affected Nodes	192.168.11.22 -						
Impact	An authenticated attacker may run arbitrary code.						
Solution	Update to 2016.74 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The dbclient and server in Dropbear SSH before 2016.74, when compiled with DEBUG_TRACE, allows local users to read process memory via the -v argument, related to a failed remote ident. Dropbear SSH < 2016.74 Multiple Vulnerabilities						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 2015.68Fixed version 2016.74Installationpath port 2400tcp						
References	http://www.openwall.com/lists/oss-security/2016/09/14/7						

CVE-2017-9078							
Risk	High		**Threat Type**	General		**CVSS**	9.3
Summary	Dropbear SSH is prone to a post-authentication root remote code execution vulnerability.						
Affected Nodes	192.168.11.22 -						
Impact	Successfully exploiting this issue might allow post-authentication root remote code execution.						
Solution	Update to Dropbear SSH version 2017.75 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled. Dropbear SSH Post-authentication root RCE Vulnerability (CVE-2017-9078)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 2015.68Fixed version 2017.75Installationpath port 2400tcp						
References	https://lists.ucc.gu.uwa.edu.au/pipermail/dropbear/2017q2/001985.html https://matt.ucc.asn.au/dropbear/CHANGES						

Risk	High		**Threat Type**	Gain a shell remotely		**CVSS**	9.3
Summary	It may be possible to make the web server crash or even execute arbitrary code by sending it a too long url through the OPTIONS method.						
Affected Nodes	192.168.11.73 -						
Impact							
Solution	Upgrade your web server.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Too long OPTIONS parameter						

Risk	**High**		**Threat Type**	Denial of Service		**CVSS**	**9.3**
Summary	The remote web server dies when an URL consisting of a long invalid string of is sent.						
Affected Nodes	192.168.11.21 -						
Impact	A attacker may use this flaw to make your server crash continually.						
Solution	Upgrade your server or firewall it.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	LiteServe URL Decoding DoS						

Risk	**High**		**Threat Type**	Denial of Service		**CVSS**	**9.3**
Summary	It seems that it is possible to lock out your printer from the network by opening a few connections and keeping them open.						
Affected Nodes	192.168.1.155 -						
Solution	Change your settings or firewall your printer.				**Solution Type**	Mitigation	
Additional Details							
CVE Description	AppSocket DoS						

<table>
<tr><th colspan="8">CVE-2017-0143</th></tr>
<tr><td><b>Risk</b></td><td><b>High</b></td><td></td><td><b>Threat Type</b></td><td>Windows Microsoft Bulletins</td><td></td><td><b>CVSS</b></td><td><b>9.3</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">This host is missing a critical security update according to Microsoft Bulletin MS17-010.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.119 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6">Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="4">The vendor has released updates. Please see the references for more information.</td><td><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148. Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://support.microsoft.com/en-us/kb/4013078
http://www.securityfocus.com/bid/96703
http://www.securityfocus.com/bid/96704
http://www.securityfocus.com/bid/96705
http://www.securityfocus.com/bid/96707
http://www.securityfocus.com/bid/96709
http://www.securityfocus.com/bid/96706
https://technet.microsoft.com/library/security/MS17-010
https://github.com/rapid7/metasploit-framework/pull/8167/files</td></tr>
</table>

CVE-2020-35606							
Risk	High		**Threat Type**	Web application abuses		**CVSS**	9.0
Summary	Webmin is prone to a remote code execution RCE vulnerability.						
Affected Nodes	192.168.11.216 -						
Solution	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.					**Solution Type**	WillNotFix
Additional Details							
CVE Description	Arbitrary command execution can occur in Webmin through 1.962. Any user authorized for the Package Updates module can execute arbitrary commands with root privileges via vectors involving %0A and %0C. NOTE: this issue exists because of an incomplete fix for CVE-2019-12840. Webmin <= 1.983 RCE Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.974Fixed version NoneInstallationpath port						
References	https://www.pentest.com.tr/exploits/Webmin-1962-PU-Escape-Bypass-Remote-Command-Execution.html						

CVE-2022-0824							
Risk	High		Threat Type	Web application abuses		CVSS	9.0
Summary	Webmin is prone to multiple vulnerabilities.						
Affected Nodes	192.168.11.216 -						
Solution	No known solution is available as of 03th March, 2022. Information regarding this issue will be updated once solution details are available.					Solution Type	NoneAvailable
Additional Details							
CVE Description	Improper Access Control to Remote Code Execution in GitHub repository webmin/webmin prior to 1.990. Webmin <= 1.984 Multiple Vulnerabilities						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.974Fixed version NoneInstallationpath port						
References	https://huntr.dev/bounties/d0049a96-de90-4b1a-9111-94de1044f295/ https://huntr.dev/bounties/f2d0389f-d7d1-4f34-9f9d-268b0a0da05e/ https://github.com/webmin/webmin/commit/eeeea3c097f5cc473770119f7ac61f1dcfa671b9 https://github.com/webmin/webmin/commit/39ea464f0c40b325decd6a5bfb7833fa4a142e38						

CVE-2015-6564							
Risk	High		Threat Type	General		CVSS	8.5
Summary	OpenSSH is prone to multiple vulnerabilities.						
Affected Nodes	192.168.11.14 -						
Impact	Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service.						
Solution	Upgrade to OpenSSH 7.0 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list. OpenSSH Multiple Vulnerabilities						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version 7.0Installationpath port 22tcp						
References	http://seclists.org/fulldisclosure/2015/Aug/54 http://openwall.com/lists/oss-security/2015/07/23/4						

CVE-2016-6380							
Risk	High		**Threat Type**	CISCO		**CVSS**	8.3
Summary	A vulnerability in the DNS forwarder functionality of Cisco IOS Softwarecould allow an unauthenticated remote attacker to cause the device to reload corrupt the information presentin the devices local DNS cache or read part of the process memory.						
Affected Nodes	192.168.30.254 -						
Impact	A successful exploit could cause the device to reload, resulting in a denial of service (DoS) condition or corruption of the local DNS cache information.						
Solution	See the referenced vendor advisory for a solution.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	The DNS forwarder in Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 3.1 through 3.15 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (data corruption or device reload) via a crafted DNS response, aka Bug ID CSCup90532. Cisco IOS Software DNS Forwarder Denial of Service Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 12.415XZFixed version See advisory						
References	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-dns						

CVE-2020-25681							
Risk	High		Threat Type	General		CVSS	8.3

Summary	Dnsmasq is prone to multiple vulnerabilities dubbed DNSpooq.		
Affected Nodes	192.168.9.170 -		
Impact	- CVE-2020-25681: This can allow a remote attacker to write arbitrary data into target device's memory that can lead to memory corruption and other unexpected behaviors on the target device. - CVE-2020-25682: This can allow a remote attacker to cause memory corruption on the target device. - CVE-2020-25683: A remote attacker, who can create valid DNS replies, could use this flaw to cause an overflow in a heap-allocated memory. This flaw could be abused to make the code execute memcpy() with a negative size in get_rdata() and cause a crash in Dnsmasq, resulting in a Denial of Service. - CVE-2020-25684: This flaw makes it easier to forge replies to an off-path attacker. - CVE-2020-25685: This flaw allows remote attackers to spoof DNS traffic that can lead to DNS cache poisoning. - CVE-2020-25686: This flaw can lead to DNS cache poisoning. - CVE-2020-25687: A remote attacker, who can create valid DNS replies, could use this flaw to cause an overflow in a heap-allocated memory. This flaw could be abused be abused to make the code execute memcpy() with a negative size in sort_rrset() and cause a crash in Dnsmasq, resulting in a Denial of Service.		
Solution	Update to version 2.83 or later.	**Solution Type**	VendorFix
Additional Details			
CVE Description	A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in forward.c:reply_query(), which is the forwarded query that matches the reply, by only using a weak hash of the query name. Due to the weak hash (CRC32 when dnsmasq is compiled without DNSSEC, SHA-1 when it is) this flaw allows an off-path attacker to find several different domains all having the same hash, substantially reducing the number of attempts they would have to perform to forge a reply and get it accepted by dnsmasq. This is in contrast with RFC5452, which specifies that the query name is one of the attributes of a query that must be used to match a reply. This flaw could be abused to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25684 the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity. Dnsmasq < 2.83 Multiple Vulnerabilities (DNSpooq)		
Detection Method	Checks if a vulnerable version is present on the target host.		
Findings	Installed version 2.80Fixed version 2.83Installationpath port 53udp		
References	https://www.jsof-tech.com/disclosures/dnspooq/ https://www.thekelleys.org.uk/dnsmasq/CHANGELOG		

<table>
<tr><th colspan="8">CVE-2014-0230</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>Web Servers</td><td></td><td>CVSS</td><td>7.8</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Apache Tomcat is prone to a denial of service DoS vulnerability.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.86 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">Successful exploitation will allow remote attackers to conduct denial of service attack.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Upgrade to version 6.0.44 or 7.0.55 or 8.0.9 or later.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle cases where an HTTP response occurs before finishing the reading of an entire request body, which allows remote attackers to cause a denial of service (thread consumption) via a series of aborted upload attempts. Apache Tomcat Denial Of Service Vulnerability - Jun15 (Windows)</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 6.0.24Fixed version 6.0.44Installationpath port 8080tcp</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://tomcat.apache.org/security-6.html
http://www.securityfocus.com/bid/74475
http://tomcat.apache.org/security-7.html
http://openwall.com/lists/oss-security/2015/04/10/1</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2012-0207</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>Denial of Service</td><td></td><td>CVSS</td><td>7.8</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">The Linux Kernel is prone to a remote denial of service DoS vulnerability.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.73 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">Successful exploitation may allow remote attackers to cause a kernel crash, denying service to legitimate users.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Upgrade to Linux Kernel version 3.0.17, 3.1.9 or 3.2.1.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">The igmp_heard_query function in net/ipv4/igmp.c in the Linux kernel before 3.2.1 allows remote attackers to cause a denial of service (divide-by-zero error and panic) via IGMP packets. Linux Kernel IGMP Remote DoS Vulnerability</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://secunia.com/advisories/47472
http://www.exploit-db.com/exploits/18378
http://www.securitytracker.com/id/1026526
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=654876
http://womble.decadent.org.uk/blog/igmp-denial-of-service-in-linux-cve-2012-0207.html
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=a8c1f65c79cbbb2f7da782d4c9d15639a9b94b27</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2017-3864</th></tr>
<tr><td><b>Risk</b></td><td><b>High</b></td><td></td><td><b>Threat Type</b></td><td>CISCO</td><td></td><td><b>CVSS</b></td><td><b>7.8</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">A vulnerability in the DHCP client implementation of Cisco IOS Software could allow an unauthenticated remote attacker to cause a denial of service DoS condition.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.30.254 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6">A successful exploit could allow the attacker to cause a reload of an affected device, resulting in a DoS condition.</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="4">See the referenced vendor advisory for a solution.</td><td><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">A vulnerability in the DHCP client implementation of Cisco IOS (12.2, 12.4, and 15.0 through 15.6) and Cisco IOS XE (3.3 through 3.7) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability occurs during the parsing of a crafted DHCP packet. An attacker could exploit this vulnerability by sending crafted DHCP packets to an affected device that is configured as a DHCP client. A successful exploit could allow the attacker to cause a reload of an affected device, resulting in a DoS condition. This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS or IOS XE Software and using a specific DHCP client configuration. Cisco Bug IDs: CSCuu43892. Cisco IOS and IOS XE Software DHCP Client Denial of Service Vulnerability</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 12.415XZFixed version See advisory</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-dhcpc</td></tr>
</table>

CVE-2015-0646							
Risk	**High**		**Threat Type**	CISCO		**CVSS**	**7.8**
Summary	A vulnerability in the TCP input module of Cisco IOS and Cisco IOS XE Software could allow an unauthenticated remote attacker to cause a memory leak and eventual reload of the affected device. The vulnerability is due to improper handling of certain crafted packet sequences used in establishing a TCP three-way handshake. An attacker could exploit this vulnerability by sending a crafted sequence of TCP packets while establishing a three-way handshake. A successful exploit could allow the attacker to cause a memory leak and eventual reload of the affected device. There are no workarounds for this vulnerability. Cisco has released software updates that address this vulnerability. Note The March 25 2015 Cisco IOS XE Software Security Advisory bundled publication includes seven Cisco Security Advisories. The advisories address vulnerabilities in Cisco IOS Software and Cisco IOS XE Software. Individual publication links are in Cisco Event Response Semiannual Cisco IOS XE Software Security Advisory Bundled Publication at the referenced links.						
Affected Nodes	192.168.30.254 -						
Impact							
Solution	See the referenced vendor advisory for a solution.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Memory leak in the TCP input module in Cisco IOS 12.2, 12.4, 15.0, 15.2, 15.3, and 15.4 and IOS XE 3.3.xXO, 3.5.xE, 3.6.xE, 3.8.xS through 3.10.xS before 3.10.5S, and 3.11.xS and 3.12.xS before 3.12.3S allows remote attackers to cause a denial of service (memory consumption or device reload) by sending crafted TCP packets over (1) IPv4 or (2) IPv6, aka Bug ID CSCum94811. Cisco IOS Software and IOS XE Software TCP Packet Memory Leak Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 12.415XZFixed version See advisory						
References	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=37433 http://tools.cisco.com/security/center/viewAlert.x?alertId=37821 http://tools.cisco.com/security/center/viewErp.x?alertId=43609 http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20150325-bundle http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html						

<table>
<tr><th colspan="8">CVE-2014-2111</th></tr>
<tr><td><b>Risk</b></td><td>High</td><td></td><td><b>Threat Type</b></td><td>CISCO</td><td></td><td><b>CVSS</b></td><td>7.8</td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">The Cisco IOS Software implementation of the Network Address Translation NAT feature contains two vulnerabilities when translating IP packets that could allow an unauthenticated remote attacker to cause a denial of service condition. Cisco has released software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities. Note The March 26 2014 Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2014 bundled publication. Individual publication links are in Cisco Event Response Semiannual Cisco IOS Software Security Advisory Bundled Publication at the referenced link.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.30.254 -</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">See the referenced vendor advisory for a solution.</td><td colspan="2"><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">The TCP Input module in Cisco IOS 12.2 through 12.4 and 15.0 through 15.4, when NAT is used, allows remote attackers to cause a denial of service (memory consumption or device reload) via crafted TCP packets, aka Bug IDs CSCuh33843 and CSCuj41494. Cisco IOS Software Network Address Translation Vulnerabilities</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 12.415XZFixed version   See advisory</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-nat
http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20140326-bundle
http://tools.cisco.com/security/center/viewAlert.x?alertId=33347
http://tools.cisco.com/security/center/viewAlert.x?alertId=33349
http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html</td></tr>
</table>

CVE-2021-28165							
Risk	High		Threat Type	Denial of Service		CVSS	7.8
Summary	Eclipse Jetty is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.11.226 -						
Impact	When using SSL/TLS with Jetty, either with HTTP/1.1, HTTP/2, or WebSocket, the server may receive an invalid large (greater than 17408) TLS frame that is incorrectly handled, causing CPU resources to eventually reach 100% usage.						
Solution	Update to version 9.4.39, 10.0.2, 11.0.2 or later. See the referenced vendor advisory for a possible mitigation.					Solution Type	VendorFix
Additional Details							
CVE Description	In Eclipse Jetty 7.2.2 to 9.4.38, 10.0.0.alpha0 to 10.0.1, and 11.0.0.alpha0 to 11.0.1, CPU usage can reach 100% upon receiving a large invalid TLS frame. Eclipse Jetty DoS Vulnerability (GHSA-26vr-8j45-3r4w) - Windows						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 7.6.9.20130131Fixed version 9.4.39Installationpath port 6143tcp						
References	https://github.com/eclipse/jetty.project/security/advisories/GHSA-26vr-8j45-3r4w						

Risk	High		Threat Type	Web Servers		CVSS	7.8
Summary	PHP Built-in WebServer is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.3.193 -						
Impact	Successful exploitation may allow remote attackers to cause the application to crash, creating a denial-of-service condition. NOTE: This NVT reports, if a similar vulnerability present in a different web-server.						
Solution	Upgrade to PHP 5.4.1RC1-DEV or 5.5.0-DEV or later.					Solution Type	VendorFix
Additional Details							
CVE Description	PHP Built-in WebServer 'Content-Length' Denial of Service Vulnerability						
References	https://bugs.php.net/bug.php?id=61461 http://www.1337day.com/exploits/17831 http://www.securityfocus.com/bid/52704 http://xforce.iss.net/xforce/xfdb/74317 http://www.exploit-db.com/exploits/18665 http://packetstormsecurity.org/files/111163/PHP-5.4.0-Denial-Of-Service.html						

Risk	**High**		**Threat Type**	Denial of Service		**CVSS**	**7.8**
Summary	The machine or a router on the way crashed when it was flooded by incorrect UDP packets.						
Affected Nodes	192.168.2.22 -						
Impact	An attacker may use this flaw to shut down this server, thus preventing you from working properly.						
Solution	If this is a FW-1, enable the antispoofing rule. Otherwise, contact your software vendor for a patch.				**Solution Type**		Mitigation
Additional Details							
CVE Description	Checkpoint Firewall-1 UDP denial of service						

CVE-2016-6515							
Risk	**High**		**Threat Type**	Denial of Service		**CVSS**	**7.8**
Summary	openssh is prone to denial of service and user enumeration vulnerabilities.						
Affected Nodes	192.168.11.14 -						
Impact	Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.						
Solution	Upgrade to OpenSSH version 7.3 or later.				**Solution Type**		VendorFix
Additional Details							
CVE Description	Sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided. OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version 7.3Installationpath port 22tcp						
References	http://www.openssh.com/txt/release-7.3 http://www.securityfocus.com/bid/92212 http://seclists.org/fulldisclosure/2016/Jul/51 https://security-tracker.debian.org/tracker/CVE-2016-6210 http://openwall.com/lists/oss-security/2016/08/01/2						

Risk	**High**		**Threat Type**	Denial of Service		**CVSS**	**7.8**
Summary	It is possible to crash the remote host by sending it malformed ICMP packets.						
Affected Nodes	192.168.1.22 -						
Impact	An attacker to make this host crash continuously, thus preventing legitimate users from using it.						
Solution	Upgrade to Linux 2.6.13 or newer, or disable SCTP support.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Malformed ICMP Packets May Cause a Denial of Service (SCTP)						
References	https://web.archive.org/web/20060718224254/http://oss.sgi.com/projects/netdev/archive/2005-07/msg00142.html						

CVE-2017-3857							
Risk	**High**		**Threat Type**	CISCO		**CVSS**	**7.8**
Summary	A vulnerability in the Layer 2 Tunneling Protocol L2TP parsing functionof Cisco IOS Software could allow an unauthenticated remote attacker to cause an affected device to reload.						
Affected Nodes	192.168.30.254 -						
Impact	A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition.						
Solution	See the referenced vendor advisory for a solution.					**Solution Type**	VendorFix
Additional Details							
CVE Description	A vulnerability in the Layer 2 Tunneling Protocol (L2TP) parsing function of Cisco IOS (12.0 through 12.4 and 15.0 through 15.6) and Cisco IOS XE (3.1 through 3.18) could allow an unauthenticated, remote attacker to cause an affected device to reload. The vulnerability is due to insufficient validation of L2TP packets. An attacker could exploit this vulnerability by sending a crafted L2TP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS or Cisco IOS XE Software if the L2TP feature is enabled for the device and the device is configured as an L2TP Version 2 (L2TPv2) or L2TP Version 3 (L2TPv3) endpoint. By default, the L2TP feature is not enabled. Cisco Bug IDs: CSCuy82078. Cisco IOS Software Layer 2 Tunneling Protocol Denial of Service Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 12.415XZFixed version See advisory						
References	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-l2tp						

CVE-2016-6384							
Risk	**High**		**Threat Type**	CISCO		**CVSS**	**7.8**
Summary	A vulnerability in the H.323 subsystem of Cisco IOS Software could allow an unauthenticated remote attacker to create a denial of service DoS condition on an affected device.						
Affected Nodes	192.168.30.254 -						
Impact	An attacker who can submit an H.323 packet designed to trigger the vulnerability could cause the affected device to crash and restart.						
Solution	See the referenced vendor advisory for a solution.			**Solution Type**	VendorFix		
Additional Details							
CVE Description	Cisco IOS 12.2 through 12.4 and 15.0 through 15.6 and IOS XE 3.1 through 3.17 and 16.2 allow remote attackers to cause a denial of service (device reload) via crafted fields in an H.323 message, aka Bug ID CSCux04257. Cisco IOS Software H.323 Message Validation Denial of Service Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 12.415XZFixed version See advisory						
References	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-h323						

<table>
<tr><th colspan="8">CVE-2010-2828</th></tr>
<tr><td><b>Risk</b></td><td>High</td><td></td><td><b>Threat Type</b></td><td>CISCO</td><td></td><td><b>CVSS</b></td><td>7.8</td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service DoS condition on a device that is running a vulnerable version of Cisco IOS Software. Cisco has released software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device. Note The September 22 2010 Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the references lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22 2010 or earlier. Individual publication links are in Cisco Event Response Semiannual Cisco IOS Software Security Advisory Bundled Publication at the references.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.30.254 -</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">See the referenced vendor advisory for a solution.</td><td colspan="2"><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><th colspan="8">Additional Details</th></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">Unspecified vulnerability in the H.323 implementation in Cisco IOS 12.1 through 12.4 and 15.0 through 15.1, and IOS XE 2.5.x before 2.5.2 and 2.6.x before 2.6.1, allows remote attackers to cause a denial of service (device reload) via crafted H.323 packets, aka Bug ID CSCtc73759. Cisco IOS Software H.323 Denial of Service Vulnerabilities</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 12.415XZFixed version   See advisory</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323
http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle
http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a315.shtml
http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html</td></tr>
</table>

Risk	**High**		**Threat Type**	Web Servers		**CVSS**	**7.5**
Summary	It was possible to kill the remote web server by requesting GET cgi-binA.AAAA...A HTTP1.0 This is known to trigger a heap overflow in some servers like CERN HTTPD.						
Affected Nodes	192.168.10.58 -						
Impact	A cracker may use this flaw to disrupt your server. It *might* also be exploitable to run malicious code on the machine.						
Solution	Ask your vendor for a patch or move to another server.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	CERN httpd CGI name heap overflow						

CVE-1999-0501							
Risk	**High**		**Threat Type**	Brute force attacks		**CVSS**	**7.5**
Summary	It was possible to login into the remote SSH server using default credentials. As the VT SSH Brute Force Logins With Default Credentials OID 1.3.6.1.4.1.25623.1.0.108013 might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.						
Affected Nodes	192.168.6.252 -						
Solution	Change the password as soon as possible.				**Solution Type**	Mitigation	
Additional Details							
CVE Description	An account on a router, firewall, or other network device has a default, null, blank, or missing password. SSH Brute Force Logins With Default Credentials Reporting						
Detection Method	Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).						
Findings	It was possible to login with the following credentials UserPasswordguestemptyno password						

CVE-1999-0710							
Risk	**High**		**Threat Type**	Web application abuses		**CVSS**	**7.5**
Summary	RedHat Linux 6.0 installs by default a squid cache manager cgi script with no restricted access permissions. This script could be used to perform a port scan from the cgi-host machine.						
Affected Nodes	192.168.1.1 -						
Solution	If you are not using the box as a Squid www proxy/cache server then uninstall the package by executing: /etc/rc.d/init.d/squid stop, rpm -e squid If you want to continue using the Squid proxy server software, make the following actions to tighten security access to the manager interface: mkdir /home/httpd/protected-cgi-bin mv /home/httpd/cgi-bin/cachemgr.cgi /home/httpd/protected-cgi-bin/ And add the following directives to /etc/httpd/conf/access.conf: # Protected cgi-bin directory for programs that # should not have public access order deny, allow deny from all allow from localhost #allow from .your_domain.com AllowOverride None Options ExecCGI and /etc/httpd/conf/srm.conf: ScriptAlias /protected-cgi-bin/ /home/httpd/protected-cgi-bin/				**Solution Type**	Mitigation	
Additional Details							
CVE Description	The Squid package in Red Hat Linux 5.2 and 6.0, and other distributions, installs cachemgr.cgi in a public web directory, which allows remote attackers to use it as an intermediary to connect to other systems. RedHat 6.0 cachemgr.cgi						

<table>
<tr><th colspan="8">CVE-2021-45951</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>Buffer overflow</td><td></td><td>CVSS</td><td>7.5</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Dnsmasq is prone to multiple vulnerabilities.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.9.170 -</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">No known solution is available as of 11th January, 2022.   Information regarding this issue will be updated once solution details are available.</td><td colspan="2">Solution Type</td><td>NoneAvailable</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">** DISPUTED ** Dnsmasq 2.86 has a heap-based buffer overflow in resize_packet (called from FuzzResizePacket and fuzz_rfc1035.c) because of the lack of a proper bounds check upon pseudo header re-insertion. NOTE: the vendor's position is that CVE-2021-45951 through CVE-2021-45957 "do not represent real vulnerabilities, to the best of our knowledge." However, a contributor states that a security patch (mentioned in 016162.html) is needed. Dnsmasq <= 2.86 Multiple Vulnerabilities</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 2.80Fixed version   NoneInstallationpath port   53udp</td></tr>
<tr><td colspan="2">References</td><td colspan="6">https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-924.yaml
https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-927.yaml
https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-929.yaml
https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-931.yaml
https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-932.yaml
https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-933.yaml
https://github.com/google/oss-fuzz-vulns/blob/main/vulns/dnsmasq/OSV-2021-935.yaml</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2001-0836</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>Gain a shell remotely</td><td></td><td>CVSS</td><td>7.5</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">It was possible to kill the web server by sending an invalid GET request with a too long User-Agent field.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.2.234 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">An attacker may exploit this vulnerability to make the web server   crash continually or even execute arbitrtay code on your system.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Upgrade your software or protect it with a filtering reverse proxy.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Buffer overflow in Oracle9iAS Web Cache 2.0.0.1 allows remote attackers to execute arbitrary code via a long HTTP GET request. HTTP User-Agent overflow</td></tr>
</table>

Risk	**High**		**Threat Type**	SMTP problems		**CVSS**	**7.5**
Summary		Some antivirus scanners dies when they process an email with a too long string without line breaks. Such a message was sent. If there is an antivirus on your MTA it might have crashed. Please check its status right now as it is not possible to do it remotely.					
Affected Nodes		192.168.11.216 -					
Impact							
Solution		Contact the vendor of the antivirus scanner to get an update.			**Solution Type**		VendorFix
Additional Details							
CVE Description		SMTP too long line					

CVE-2020-11945							
Risk	**High**		**Threat Type**	Web application abuses		**CVSS**	**7.5**
Summary		Squid is prone to multiple vulnerabilities in the HTTP Digest authentication.					
Affected Nodes		192.168.1.251 -					
Solution		Update to version 4.11, 5.0.2 or later.			**Solution Type**		VendorFix
Additional Details							
CVE Description		An issue was discovered in Squid before 5.0.2. A remote attacker can replay a sniffed Digest Authentication nonce to gain access to resources that are otherwise forbidden. This occurs because the attacker can overflow the nonce reference counter (a short integer). Remote code execution may occur if the pooled token credentials are freed (instead of replayed as valid credentials). Squid Proxy Cache Security Update Advisory SQUID-2020:4					
Detection Method		Checks if a vulnerable version is present on the target host.					
Findings		Installed version 3.5.20Fixed version 4.11					
References		http://www.squid-cache.org/Advisories/SQUID-2020_4.txt					

Risk	**High**		**Threat Type**	Denial of Service		**CVSS**	**7.5**
Summary	It was possible to kill the web server by sending an invalid request with an incomplete Basic authentication.						
Affected Nodes	192.168.3.193 -						
Impact	An attacker may exploit this vulnerability to make the web server crash continually or even execute arbirtray code on your system.						
Solution	Upgrade your software or protect it with a filtering reverse proxy.			**Solution Type**	VendorFix		
Additional Details							
CVE Description	Incomplete basic authentication DoS						

CVE-2001-0361

Risk	**High**		**Threat Type**	General		**CVSS**	**7.5**
Summary	The host is running SSH and is providing accepting one or more deprecated versions of the SSH protocol which have known cryptograhic flaws.						
Affected Nodes	192.168.4.1 -						
Impact	Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.						
Solution	Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.			**Solution Type**	VendorFix		
Additional Details							
CVE Description	The SSH-1 protocol allows remote servers to conduct man-in-the-middle attacks and replay a client challenge response to a target server by creating a Session ID that matches the Session ID of the target, but which uses a public key pair that is weaker than the target's public key, which allows the attacker to compute the corresponding private key and use the target's Session ID with the compromised key pair to masquerade as the target. Deprecated SSH-1 Protocol Detection						
Detection Method							
Findings	The service is providing accepting the following deprecated versions of the SSH protocol which have known cryptograhic flaws1.5						
References	http://www.kb.cert.org/vuls/id/684820 http://xforce.iss.net/xforce/xfdb/6603						

CVE-2002-1061							
Risk	High		Threat Type	Denial of Service		CVSS	7.5
Summary	It was possible to kill the web server by sending an invalid request with a too long HTTP method field						
Affected Nodes	192.168.3.193 -						
Impact	An attacker may exploit this vulnerability to make the web server crash continually or even execute arbirtray code on the affected system.						
Solution	Upgrade your software or protect it with a filtering reverse proxy.				Solution Type	VendorFix	
Additional Details							
CVE Description	Multiple buffer overflows in Thomas Hauck Jana Server 2.x through 2.2.1, and 1.4.6 and earlier, allow remote attackers to cause a denial of service and possibly execute arbitrary code via (1) an HTTP GET request with a long major version number, (2) an HTTP GET request to the HTTP proxy on port 3128 with a long major version number, (3) a long OK reply from a POP3 server, and (4) a long SMTP server response. HTTP method overflow						

Risk	High		Threat Type	Gain a shell remotely		CVSS	7.5
Summary	It was possible to kill the web server by sending an invalid request with a too long header From If-Modified-Since Referer or Content-Type						
Affected Nodes	192.168.1.103 -						
Impact	An attacker may exploit this vulnerability to make your web server crash continually or even execute arbitrary code on the target system.						
Solution	Upgrade your software or protect it with a filtering reverse proxy.				Solution Type	VendorFix	
Additional Details							
CVE Description	HTTP 1.0 header overflow						

<table>
<tr><th colspan="8">CVE-2019-12519</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>Web application abuses</td><td></td><td>CVSS</td><td>7.5</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Squid is prone to multiple vulnerabilities.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.1.251 -</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Update to version 4.11, 5.0.2 or later.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">An issue was discovered in Squid through 4.7. When Squid is parsing ESI, it keeps the ESI elements in ESIContext. ESIContext contains a buffer for holding a stack of ESIElements. When a new ESIElement is parsed, it is added via addStackElement. addStackElement has a check for the number of elements in this buffer, but it's off by 1, leading to a Heap Overflow of 1 element. The overflow is within the same structure so it can't affect adjacent memory blocks, and thus just leads to a crash while processing. Squid Proxy Cache Security Update Advisory SQUID-2019:12</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 3.5.20Fixed version 4.11</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://www.squid-cache.org/Advisories/SQUID-2019_12.txt
https://gitlab.com/jeriko.one/security/-/blob/master/squid/CVEs/CVE-2019-12519.txt
https://gitlab.com/jeriko.one/security/-/blob/master/squid/CVEs/CVE-2019-12521.txt</td></tr>
</table>

CVE-1999-0519							
Risk	High		**Threat Type**	Windows		**CVSS**	7.5
Summary	Microsoft Windows is prone to an authentication bypass vulnerability via SMBNETBIOS.						
Affected Nodes	192.168.11.110 -						
Impact	Successful exploitation could allow attackers to use shares to cause the system to crash.						
Solution	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. A workaround is to, - Disable null session login. - Remove the share. - Enable passwords on the share.				**Solution Type**	WillNotFix	
Additional Details							
CVE Description	A NETBIOS/SMB share password is the default, null, or missing. Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability						
Findings	It was possible to login at the share IPC with an empty login and password.						
References	http://xforce.iss.net/xforce/xfdb/2 http://seclab.cs.ucdavis.edu/projects/testing/vulner/38.html						

CVE-2002-1061							
Risk	High		**Threat Type**	Gain a shell remotely		**CVSS**	7.5
Summary	It was possible to kill the web server by sending an invalid GET request with a too long HTTP version field.						
Affected Nodes	192.168.11.73 -						
Impact	An attacker may exploit this vulnerability to make the web server crash continually or even execute arbitrtay code on the affected system.						
Solution	Upgrade your software or protect it with a filtering reverse proxy.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Multiple buffer overflows in Thomas Hauck Jana Server 2.x through 2.2.1, and 1.4.6 and earlier, allow remote attackers to cause a denial of service and possibly execute arbitrary code via (1) an HTTP GET request with a long major version number, (2) an HTTP GET request to the HTTP proxy on port 3128 with a long major version number, (3) a long OK reply from a POP3 server, and (4) a long SMTP server response. HTTP version number overflow						

<table>
<tr><th colspan="8">CVE-2014-1692</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>General</td><td></td><td>CVSS</td><td>7.5</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">OpenSSH is prone to a remote memory-corruption vulnerability.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.76 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">An attacker can exploit this issue to execute arbitrary code in context of the application. Failed exploits may result in denial-of-service conditions.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Updates are available. Please see the references for more information.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition. OpenSSH 'schnorr.c' Remote Memory Corruption Vulnerability</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 6.2Fixed version See referencesInstallationpath port 22tcp</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://www.securityfocus.com/bid/65230</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-1999-1072</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>Web application abuses</td><td></td><td>CVSS</td><td>7.5</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Some of the following dangerous CGIs were found. By default this script only checks for this CGIs within the cgi-bin directory. You can change this behavior with the script preference to check all detected CGI directories.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.31 -</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Please take the time to visit cve.mitre.org and check the associated CVE ID for each cgi found. If you are running a vulnerable version, then delete or upgrade the CGI.</td><td colspan="2">Solution Type</td><td>Mitigation</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Cross-site scripting vulnerability in YaBB.cgi for Yet Another Bulletin Board (YaBB) 1 Gold SP1 and earlier allows remote attackers to execute arbitrary script as other web site visitors via script in the num parameter, which is not filtered in the resulting error message. Various dangerous cgi scripts</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6"></td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">The following dangerous CGI scripts were foundhttps192.168.11.31cgi-binservice.cgi CVE-2002-0346</td></tr>
<tr><td colspan="2">References</td><td colspan="6"></td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2011-3190</th></tr>
<tr><td><b>Risk</b></td><td><b>High</b></td><td></td><td><b>Threat Type</b></td><td>Web Servers</td><td></td><td><b>CVSS</b></td><td><b>7.5</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">Apache Tomcat is prone to a security-bypass vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.86 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6">Successful exploits will allow attackers to bypass certain security restrictions.</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="4">Updates are available. Please see the references for more information.</td><td><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">Certain AJP protocol connector implementations in Apache Tomcat 7.0.0 through 7.0.20, 6.0.0 through 6.0.33, 5.5.0 through 5.5.33, and possibly other versions allow remote attackers to spoof AJP requests, bypass authentication, and obtain sensitive information by causing the connector to interpret a request body as a new request. Apache Tomcat AJP Protocol Security Bypass Vulnerability</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 6.0.24Fixed version 5.5.346.0.347.0.21Installationpath port 8080tcp</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">http://www.securityfocus.com/bid/49353
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html
http://tomcat.apache.org/security-7.html</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2016-1908</th></tr>
<tr><td><b>Risk</b></td><td><b>High</b></td><td></td><td><b>Threat Type</b></td><td>General</td><td></td><td><b>CVSS</b></td><td><b>7.5</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">openssh is prone to a security bypass vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.14 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6">Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="4">Upgrade to OpenSSH version 7.2 or later.</td><td><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server. OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 6.6.1Fixed version 7.2Installationpath port 22tcp</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">http://openwall.com/lists/oss-security/2016/01/15/13
http://www.securityfocus.com/bid/84427
https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4
http://www.openssh.com/txt/release-7.2
https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6fa0db113c71e234416c
https://bugzilla.redhat.com/show_bug.cgi?id=1298741</td></tr>
</table>

CVE-2016-10009							
Risk	**High**		**Threat Type**	General		**CVSS**	**7.5**
Summary	openssh is prone to multiple vulnerabilities.						
Affected Nodes	192.168.11.14 -						
Impact	Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.						
Solution	Upgrade to OpenSSH version 7.4 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures. OpenSSH Multiple Vulnerabilities Jan17 (Linux)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version 7.4Installationpath port 22tcp						
References	https://www.openssh.com/txt/release-7.4 http://www.securityfocus.com/bid/94968 http://www.securityfocus.com/bid/94972 http://www.securityfocus.com/bid/94977 http://www.securityfocus.com/bid/94975 http://www.openwall.com/lists/oss-security/2016/12/19/2 http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e933e6b931de1d16737						

CVE-2019-12528							
Risk	High		Threat Type	Web application abuses		CVSS	7.5
Summary	Squid is prone to multiple vulnerabilities.						
Affected Nodes	192.168.1.251 -						
Solution	Update to version 4.10 or later.				Solution Type	VendorFix	
Additional Details							
CVE Description	An issue was discovered in Squid before 4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy. Squid Proxy Cache Multiple Security Update Advisories SQUID-2020:1, SQUID-2020:2, SQUID-2020:3						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.10						
References	http://www.squid-cache.org/Advisories/SQUID-2020_1.txt http://www.squid-cache.org/Advisories/SQUID-2020_2.txt http://www.squid-cache.org/Advisories/SQUID-2020_3.txt						

CVE-1999-0071							
Risk	High		Threat Type	Gain a shell remotely		CVSS	7.5
Summary	It was possible to kill the web server by sending an invalid request with a too long Cookie name or value.						
Affected Nodes	192.168.11.73 -						
Impact	A cracker may exploit this vulnerability to make your web server crash continually or even execute arbitrary code on your system.						
Solution	Upgrade your software or protect it with a filtering reverse proxy.				Solution Type	VendorFix	
Additional Details							
CVE Description	Apache httpd cookie buffer overflow for versions 1.1.1 and earlier. HTTP Cookie overflow						

CVE-2019-12525							
Risk	High		Threat Type	Denial of Service		CVSS	7.5
Summary	Squid is prone to a denial of service vulnerability due to incorrect buffer management when processing HTTP Digest Authentication credentials.						
Affected Nodes	192.168.1.251 -						
Solution	Update to version 4.8 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	An issue was discovered in Squid 3.3.9 through 3.5.28 and 4.x through 4.7. When Squid is configured to use Digest authentication, it parses the header Proxy-Authorization. It searches for certain tokens such as domain, uri, and qop. Squid checks if this token's value starts with a quote and ends with one. If so, it performs a memcpy of its length minus 2. Squid never checks whether the value is just a single quote (which would satisfy its requirements), leading to a memcpy of its length minus 1. Squid Proxy Cache Security Update Advisory SQUID-2018:3						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.8						
References	http://www.squid-cache.org/Advisories/SQUID-2019_3.txt						

CVE-2019-12526							
Risk	High		Threat Type	Web application abuses		CVSS	7.5
Summary	Squid is prone to multiple vulnerabilities.						
Affected Nodes	192.168.1.251 -						
Solution	Update to version 4.9 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	An issue was discovered in Squid 3.x and 4.x through 4.8. It allows attackers to smuggle HTTP requests through frontend software to a Squid instance that splits the HTTP Request pipeline differently. The resulting Response messages corrupt caches (between a client and Squid) with attacker-controlled content at arbitrary URLs. Effects are isolated to software between the attacker client and Squid. There are no effects on Squid itself, nor on any upstream servers. The issue is related to a request header containing whitespace between a header name and a colon. Squid Proxy Cache Multiple Security Update Advisories (SQUID-2019:7, SQUID-2019:8, SQUID-2019:10)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.9						
References	http://www.squid-cache.org/Advisories/SQUID-2019_7.txt http://www.squid-cache.org/Advisories/SQUID-2019_8.txt http://www.squid-cache.org/Advisories/SQUID-2019_10.txt						

CVE-2019-12520							
Risk	**High**		**Threat Type**	Web application abuses		**CVSS**	**7.5**
Summary	Squid is prone to multiple vulnerabilities.						
Affected Nodes	192.168.1.251 -						
Impact	A remote client can: - deliver crafted URLs to bypass cache manager security controls and retrieve confidential details about the proxy and traffic it is handling. - deliver crafted URLs which cause arbitrary content from one origin server to be stored in cache as URLs within another origin. This opens a window of opportunity for clients to be tricked into fetching and XSS execution of that content via side channels.						
Solution	Update to version 4.8 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	An issue was discovered in Squid through 4.7 and 5. When receiving a request, Squid checks its cache to see if it can serve up a response. It does this by making a MD5 hash of the absolute URL of the request. If found, it servers the request. The absolute URL can include the decoded UserInfo (username and password) for certain protocols. This decoded info is prepended to the domain. This allows an attacker to provide a username that has special characters to delimit the domain, and treat the rest of the URL as a path or query string. An attacker could first make a request to their domain using an encoded username, then when a request for the target domain comes in that decodes to the exact URL, it will serve the attacker's HTML instead of the real HTML. On Squid servers that also act as reverse proxies, this allows an attacker to gain access to features that only reverse proxies can use, such as ESI. Squid Proxy Cache 3.5.18 - 3.5.28 / 4.0.10 - 4.7 Multiple Vulnerabilities (SQUID-2019:4)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.8Installationpath port 3128tcp						
References	https://gitlab.com/jeriko.one/security/-/blob/master/squid/CVEs/CVE-2019-12520.txt https://gitlab.com/jeriko.one/security/-/blob/master/squid/CVEs/CVE-2019-12524.txt http://www.squid-cache.org/Advisories/SQUID-2019_4.txt						

CVE-2015-8325							
Risk	High		Threat Type	General		CVSS	7.2
Summary	openssh is prone to a privilege escalation vulnerability.						
Affected Nodes	192.168.11.14 -						
Impact	Successfully exploiting this issue will allow local users to gain privileges.						
Solution	Upgrade to OpenSSH version 7.2p2-3 or later.			Solution Type	VendorFix		
Additional Details							
CVE Description	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable. OpenSSH Privilege Escalation Vulnerability - May16						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version 7.2p2-3Installationpath port 22tcp						
References	https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755						

CVE-2017-4902							
Risk	High		Threat Type	General		CVSS	7.2
Summary	VMware ESXi Workstation and Fusion updates address critical and moderatesecurity issues.ESXi has a heap buffer overflow and uninitialized stack memory usage in SVGA. These issues may allow a guest to execute code on the host.						
Affected Nodes	192.168.11.14 -						
Solution	Apply the missing patch(es).			Solution Type	VendorFix		
Additional Details							
CVE Description	The XHCI controller in VMware ESXi 6.5 without patch ESXi650-201703410-SG, 6.0 U3 without patch ESXi600-201703401-SG, 6.0 U2 without patch ESXi600-201703403-SG, 6.0 U1 without patch ESXi600-201703402-SG, and 5.5 without patch ESXi550-201703401-SG; Workstation Pro / Player 12.x prior to 12.5.5; and Fusion Pro / Fusion 8.x prior to 8.5.6 has uninitialized memory usage. This issue may allow a guest to execute code on the host. The issue is reduced to a Denial of Service of the guest on ESXi 5.5. VMSA-2017-0006: VMware ESXi updates address critical and moderate security issues (remote check)						
Detection Method	Check the build number						
Findings	ESXi Version 6.0.0Detected Build 2494585Fixed Build 5224934						
References	http://www.vmware.com/security/advisories/VMSA-2017-0006.html						

Risk	**High**		**Threat Type**	Denial of Service		**CVSS**	**7.2**
Summary	This script sends the 42.zip recursive archive to the mail server. If there is an antivirus filter it may start eating huge amounts of CPU or memory.						
Affected Nodes	192.168.11.216 -						
Impact							
Solution	Reconfigure your antivirus / upgrade it.				**Solution Type**	Mitigation	
Additional Details							
CVE Description	SMTP antivirus scanner DoS						
Findings	The file 42.zip was sent 2 times. If there is an antivirus in your MTA it might have crashed. Please check its status right now as it is not possible to do so remotely.						

CVE-2013-5745							
Risk	**High**		**Threat Type**	Denial of Service		**CVSS**	**7.1**
Summary	Vino VNC Server is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.11.76 -						
Impact	Successful exploitation will allow attacker to cause a denial of service. Additionally, after the failure condition has occurred, the log file (~/.xsession-errors) grows quickly.						
Solution	Upgrade to version 3.7.4 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	The vino_server_client_data_pending function in vino-server.c in GNOME Vino 2.26.1, 2.32.1, 3.7.3, and earlier, and 3.8 when encryption is disabled, does not properly clear client data when an error causes the connection to close during authentication, which allows remote attackers to cause a denial of service (infinite loop, CPU and disk consumption) via multiple crafted requests during authentication. Vino VNC Server Remote Denial Of Service Vulnerability						
Detection Method	Send crafted request and check is it vulnerable to DoS or not.						
References	http://xforce.iss.net/xforce/xfdb/87155 http://www.exploit-db.com/exploits/28338 https://bugzilla.gnome.org/show_bug.cgi?id=707905 https://bugzilla.gnome.org/show_bug.cgi?id=641811 https://access.redhat.com/security/cve/CVE-2013-5745						

Risk	High		Threat Type	Denial of Service		CVSS	7.1
Summary	It was possible to kill the web server by sending a MS-DOS device names in an HTTP request.						
Affected Nodes	192.168.3.193 -						
Impact	An attacker may use this flaw to prevent this host from performing its job properly.						
Solution	Upgrade your web server to the latest version.				Solution Type	VendorFix	
Additional Details							
CVE Description	Abyss httpd DoS						

CVE-2020-24606							
Risk	High		Threat Type	Denial of Service		CVSS	7.1
Summary	Squid is prone to a denial of service vulnerability when processing Cache Digest responses.						
Affected Nodes	192.168.1.251 -						
Impact	This problem allows a trusted peer to perform a Denial of Service by consuming all available CPU cycles on the machine running Squid when handling a crafted Cache Digest response message. This attack is limited to Squid using cache_peer with cache digests feature.						
Solution	Update to version 4.13, 5.0.4 or later.				Solution Type	VendorFix	
Additional Details							
CVE Description	Squid before 4.13 and 5.x before 5.0.4 allows a trusted peer to perform Denial of Service by consuming all available CPU cycles during handling of a crafted Cache Digest response message. This only occurs when cache_peer is used with the cache digests feature. The problem exists because peerDigestHandleReply() livelocking in peer_digest.cc mishandles EOF. Squid Proxy Cache Security Update Advisory SQUID-2020:9						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.13						
References	https://github.com/squid-cache/squid/security/advisories/GHSA-vvj7-xjgq-g2jg						

CVE-2012-3950							
Risk	**High**		**Threat Type**	CISCO		**CVSS**	**7.1**
Summary	Cisco IOS Software contains a vulnerability in the Intrusion Prevention System IPS feature that could allow an unauthenticated remote attacker to cause a reload of an affected device if specific Cisco IOS IPS configurations exist. Cisco has released software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. Note The September 26 2012 Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2012 bundled publication. Individual publication links are in Cisco Event Response Semi-Annual Cisco IOS Software Security Advisory Bundled Publication at the referenced link.						
Affected Nodes	192.168.30.254 -						
Solution	See the referenced vendor advisory for a solution.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The Intrusion Prevention System (IPS) feature in Cisco IOS 12.3 through 12.4 and 15.0 through 15.2, in certain configurations of enabled categories and missing signatures, allows remote attackers to cause a denial of service (device reload) via DNS packets, aka Bug ID CSCtw55976. Cisco IOS Software Intrusion Prevention System Denial of Service Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 12.415XZFixed version See advisory						
References	http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20120926-bundle http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html						

CVE-2016-6393							
Risk	High		Threat Type	CISCO		CVSS	7.1
Summary	A vulnerability in the Authentication Authorization and Accounting AAAservice for remote Secure Shell Host SSH connections to the device for Cisco IOS Software could allow an unauthenticated remote attacker to cause the vulnerable device to reload.						
Affected Nodes	192.168.30.254 -						
Impact	An exploit could allow the attacker to cause a denial of service (DoS) condition.						
Solution	See the referenced vendor advisory for a solution.				Solution Type	VendorFix	
Additional Details							
CVE Description	The AAA service in Cisco IOS 12.0 through 12.4 and 15.0 through 15.6 and IOS XE 2.1 through 3.18 and 16.2 allows remote attackers to cause a denial of service (device reload) via a failed SSH connection attempt that is mishandled during generation of an error-log message, aka Bug ID CSCuy87667. Cisco IOS Software AAA Login Denial of Service Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 12.415XZFixed version See advisory						
References	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-aaados						

Risk	High		Threat Type	Gain a shell remotely		CVSS	6.9
Summary	The remote web server seems to be vulnerable to a format string attack on HTTP headers names.						
Affected Nodes	192.168.3.193 -						
Impact	An attacker might use this flaw to make it crash or even execute arbitrary code on this host.						
Solution	Upgrade your software or contact your vendor and inform him of this vulnerability.				Solution Type	VendorFix	
Additional Details							
CVE Description	Format string on HTTP header name						

Risk	**High**		**Threat Type**	Gain a shell remotely		**CVSS**	**6.9**
Summary	The remote web server seems to be vulnerable to a format string attack on the method name.						
Affected Nodes	192.168.10.53 -						
Impact	An attacker might use this flaw to make it crash or even execute arbitrary code on this host.						
Solution	Upgrade your software or contact your vendor and inform him of this vulnerability.				**Solution Type**		VendorFix
Additional Details							
CVE Description	Format string on HTTP method name						

Risk	**High**		**Threat Type**	Gain a shell remotely		**CVSS**	**6.9**
Summary	The remote web server seems to be vulnerable to a format string attack on HTTP 1.0 header value.						
Affected Nodes	192.168.11.21 -						
Impact	An attacker might use this flaw to make it crash or even execute arbitrary code on this host.						
Solution	Upgrade your software or contact your vendor and inform him of this vulnerability.				**Solution Type**		VendorFix
Additional Details							
CVE Description	Format string on HTTP header value						

CVE-2011-1499

Risk	**High**		**Threat Type**	Web application abuses		**CVSS**	**6.8**
Summary	Tinyproxy is prone to multiple security-bypass vulnerabilities.						
Affected Nodes	192.168.13.48 -						
Impact	Successful exploits will allow attackers to bypass certain security restrictions and gain unauthorized access to the application. This may aid in further attacks.						
Solution	Upgrade to Tinyproxy 1.8.3 or newer.				**Solution Type**		VendorFix
Additional Details							
CVE Description	Acl.c in Tinyproxy before 1.8.3, when an Allow configuration setting specifies a CIDR block, permits TCP connections from all IP addresses, which makes it easier for remote attackers to hide the origin of web traffic by leveraging the open HTTP proxy server. Tinyproxy < 1.8.3 Multiple Security Bypass Vulnerabilities						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.8.2Fixed version 1.8.3						
References	http://www.securityfocus.com/bid/47276 http://www.securityfocus.com/bid/47715						

CVE-2015-7547

Risk	**High**		**Threat Type**	General		**CVSS**	**6.8**
Summary	VMware product updates address a critical glibc security vulnerability.						
Affected Nodes	192.168.11.14 -						
Solution	Apply the missing patch(es).				**Solution Type**		VendorFix
Additional Details							
CVE Description	Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module. VMSA-2016-0002: VMware product updates address a critical glibc security vulnerability (remote check)						
Detection Method	Check the build number.						
Findings	ESXi Version 6.0.0Detected Build 2494585Fixed Build 3568940						
References	http://www.vmware.com/security/advisories/VMSA-2016-0002.html						

CVE-2020-15778							
Risk	**High**		**Threat Type**	General		**CVSS**	**6.8**
Summary	OpenSSH is prone to a remote code execution vulnerability.						
Affected Nodes	192.168.11.14 -						
Impact	Successful exploitation would allow an attacker to execute arbitrary code on the target machine.						
Solution	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.				**Solution Type**		WillNotFix
Additional Details							
CVE Description	** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows." OpenSSH <= 8.6 Command Injection Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version NoneInstallationpath port 22tcp						
References	https://github.com/cpandya2909/CVE-2020-15778/						

CVE-2020-36254							
Risk	High		**Threat Type**	General		**CVSS**	**6.8**
Summary	Dropbear is mishandling the filename of . or an empty filename.						
Affected Nodes	192.168.11.22 -						
Impact	Successful exploitation would allow an attacker to modify the permissions of the target directory on the client side.						
Solution	Update Dropbear to version 2020.79 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Scp.c in Dropbear before 2020.79 mishandles the filename of . or an empty filename, a related issue to CVE-2018-20685. Dropbear < 2020.79 Mishandling Filenames Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 2015.68Fixed version 2020.79Installationpath port 2400tcp						
References	https://github.com/mkj/dropbear/commit/8f8a3dff705fad774a10864a2e3dbcfa9779ceff https://matt.ucc.asn.au/dropbear/CHANGES						

CVE-2014-1820							
Risk	High		**Threat Type**	Windows Microsoft Bulletins		**CVSS**	**6.8**
Summary	This host is missing an important security update according to Microsoft Bulletin MS14-044.						
Affected Nodes	192.168.11.110 -						
Impact	Successful exploitation will allow remote attackers to cause a Denial of Service or elevation of privilege.						
Solution	The vendor has released updates. Please see the references for more information.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Microsoft SQL Server 2008 SP3, 2008 R2 SP2, and 2012 SP1 does not properly control use of stack memory for processing of T-SQL batch commands, which allows remote authenticated users to cause a denial of service (daemon hang) via a crafted T-SQL statement, aka "Microsoft SQL Server Stack Overrun Vulnerability." Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) - Remote						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 12.0.2000.0Vulnerable range 12.0.2000 - 12.0.2253 12.0.2300 - 12.0.2380						
References	https://technet.microsoft.com/library/security/MS14-044						

CVE-2016-6816

Risk	**High**		**Threat Type**	Web Servers		**CVSS**	**6.8**

Summary	Apache Tomcat is prone to an information disclosure vulnerability.		
Affected Nodes	192.168.11.86 -		
Impact	Successful exploitation will allow remote attackers to poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own.		
Solution	Upgrade to version 9.0.0.M13, 8.5.8, 8.0.39, 7.0.73, 6.0.48 or later.	**Solution Type**	VendorFix

Additional Details

CVE Description	The code in Apache Tomcat 9.0.0.M1 to 9.0.0.M11, 8.5.0 to 8.5.6, 8.0.0.RC1 to 8.0.38, 7.0.0 to 7.0.72, and 6.0.0 to 6.0.47 that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own. Apache Tomcat HTTP Request Line Information Disclosure Vulnerability (Windows)
Detection Method	Checks if a vulnerable version is present on the target host.
Findings	Installed version 6.0.24Fixed version 6.0.48Installationpath port 8080tcp
References	https://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.48 http://www.securityfocus.com/bid/94461 https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.73 https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.39 https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.8 https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M13 https://qnalist.com/questions/7885204/security-cve-2016-6816-apache-tomcat-information-disclosure

CVE-2021-31760							
Risk	High		**Threat Type**	Web application abuses		**CVSS**	6.8
Summary	Webmin is prone to multiple vulnerabilities.						
Affected Nodes	192.168.11.216 -						
Solution	No known solution is available as of 29th October, 2021. Information regarding this issue will be updated once solution details are available.				**Solution Type**	NoneAvailable	
Additional Details							
CVE Description	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to create a privileged user through Webmin's add users feature, and then get a reverse shell through Webmin's running process feature. Webmin <= 1.980 Multiple Vulnerabilities						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.974Fixed version NoneInstallationpath port						
References	https://github.com/Mesh3l911/CVE-2021-31760 https://github.com/Mesh3l911/CVE-2021-31761 https://github.com/Mesh3l911/CVE-2021-31762						

CVE-2013-2067							
Risk	High		**Threat Type**	Web Servers		**CVSS**	6.8
Summary	Apache Tomcat is prone to a session fixation vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow attackers to conduct session fixation attacks to hijack the target user's session.						
Solution	Update to version 6.0.37, 7.0.33 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Java/org/apache/catalina/authenticator/FormAuthenticator.java in the form authentication feature in Apache Tomcat 6.0.21 through 6.0.36 and 7.x before 7.0.33 does not properly handle the relationships between authentication requirements and sessions, which allows remote attackers to inject a request into a session by sending this request during completion of the login form, a variant of a session fixation attack. Apache Tomcat Session Fixation Vulnerability (Nov 2012) - Windows						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.377.0.33Installationpath port 8080tcp						
References	http://xforce.iss.net/xforce/xfdb/84154 http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-7.html http://svn.apache.org/viewvc?view=revision&revision=1417891 http://svn.apache.org/viewvc?view=revision&revision=1408044						

CVE-2021-41987							
Risk	**High**		**Threat Type**	Web application abuses		**CVSS**	**6.8**
Summary	MikroTik RouterOS is prone to a remote code execution RCE vulnerability.						
Affected Nodes	192.168.11.62 -						
Solution	Update to version 6.48.6, 6.49.1, 7.1 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	In the SCEP Server of RouterOS in certain Mikrotik products, an attacker can trigger a heap-based buffer overflow that leads to remote code execution. The attacker must know the scep_server_name value. This affects RouterOS 6.46.8, 6.47.9, and 6.47.10. MikroTik RouterOS RCE Vulnerability (CVE-2021-41987)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.47.10Fixed version 6.48.6						
References	https://teamt5.org/en/posts/vulnerability-mikrotik-cve-2021-41987/						

CVE-2020-15049							
Risk	**High**		**Threat Type**	Web application abuses		**CVSS**	**6.5**
Summary	Squid is prone to a cache poisoning vulnerability.						
Affected Nodes	192.168.1.251 -						
Solution	Update to version 4.12, 5.0.3 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	An issue was discovered in http/ContentLengthInterpreter.cc in Squid before 4.12 and 5.x before 5.0.3. A Request Smuggling and Poisoning attack can succeed against the HTTP cache. The client sends an HTTP request with a Content-Length header containing "+\ "-" or an uncommon shell whitespace character prefix to the length field-value. Squid Proxy Cache Security Update Advisory SQUID-2020:7						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.12						
References	https://github.com/squid-cache/squid/security/advisories/GHSA-qf3v-rc95-96j5						

CVE-2015-6933							
Risk	**High**		**Threat Type**	General		**CVSS**	**6.5**
Summary	VMware ESXi Fusion Player and Workstation updates address important guest privilege escalation vulnerability						
Affected Nodes	192.168.11.14 -						
Solution	Apply the missing patch(es).				**Solution Type**	VendorFix	
Additional Details							
CVE Description	The VMware Tools HGFS (aka Shared Folders) implementation in VMware Workstation 11.x before 11.1.2, VMware Player 7.x before 7.1.2, VMware Fusion 7.x before 7.1.2, and VMware ESXi 5.0 through 6.0 allows Windows guest OS users to gain guest OS privileges or cause a denial of service (guest OS kernel memory corruption) via unspecified vectors. VMSA-2016-0001 VMware ESXi, Fusion, Player, and Workstation updates address important guest privilege escalation vulnerability (remote check)						
Detection Method	Check the build number						
Findings	ESXi Version 6.0.0Detected Build 2494585Fixed Build 3341439						
References	http://www.vmware.com/security/advisories/VMSA-2016-0001.html						

CVE-2016-0714							
Risk	High		Threat Type	Web Servers		CVSS	6.5
Summary	Apache Tomcat is prone to a security manager bypass vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote authenticated users to bypass intended SecurityManager restrictions and execute arbitrary code in a privileged context and read arbitrary HTTP requests, and consequently discover session ID values.						
Solution	Upgrade to version 6.0.45 or 7.0.68 or 8.0.32 or 9.0.0.M3 or later.				Solution Type		VendorFix
Additional Details							
CVE Description	Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 does not place org.apache.catalina.manager.StatusManagerServlet on the org/apache/catalina/core/RestrictedServlets.properties list, which allows remote authenticated users to bypass intended SecurityManager restrictions and read arbitrary HTTP requests, and consequently discover session ID values, via a crafted web application. Apache Tomcat Security Manager Bypass Vulnerability - 01 - Feb16 (Windows)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.45Installationpath port 8080tcp						
References	http://tomcat.apache.org/security-9.html http://www.securityfocus.com/bid/83324 http://www.securityfocus.com/bid/83327 http://tomcat.apache.org/security-8.html http://tomcat.apache.org/security-7.html						

CVE-1999-0497							
Risk	High		Threat Type	FTP		CVSS	6.4
Summary	Reports if the remote FTP Server allows anonymous logins.						
Affected Nodes	192.168.11.64 -						
Impact	Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to: - gain access to sensitive files - upload or delete files.						
Solution	If you do not want to share files, you should disable anonymous logins.				Solution Type		Mitigation
Additional Details							
CVE Description	Anonymous FTP is enabled. Anonymous FTP Login Reporting						
Findings	It was possible to login to the remote FTP service with the following anonymous accountsanonymousanonymousexample.comftpanonymousexample.com						
References							

Risk	High		Threat Type	SSL and TLS		CVSS	6.4
Summary	a server with SSLTLS is prone to an information disclosure vulnerability.						
Affected Nodes	192.168.3.253 -						
Impact							
Solution	Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.				Solution Type	Mitigation	
Additional Details							
CVE Description	SSL/TLS: Missing `secure` Cookie Attribute						
Findings	The cookiesSet-Cookie AIROSSESSIONIDreplaced Path Version1are missing the secure attribute.						
References	https://www.owasp.org/index.php/SecureFlag http://www.ietf.org/rfc/rfc2965.txt https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)						

CVE-2014-0227							
Risk	High		Threat Type	Web Servers		CVSS	6.4
Summary	Apache Tomcat is prone to denial of service DoS vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to perform a denial of service attack by streaming an unlimited quantity of data, leading to excessive consumption of system resources.						
Solution	Update to version 6.0.42, 7.0.55, 8.0.9 or later.				Solution Type	VendorFix	
Additional Details							
CVE Description	Java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat 6.x before 6.0.42, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle attempts to continue reading data after an error has occurred, which allows remote attackers to conduct HTTP request smuggling attacks or cause a denial of service (resource consumption) by streaming data with malformed chunked transfer coding. Apache Tomcat DoS Vulnerability (Mar 2015) - Windows						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.42Installationpath port 8080tcp						
References	http://tomcat.apache.org/security-8.html http://tomcat.apache.org/security-7.html http://tomcat.apache.org/security-6.html http://archives.neohapsis.com/archives/bugtraq/2015-02/0067.html						

<table>
<tr><th colspan="8">CVE-2010-2227</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>Web Servers</td><td></td><td>CVSS</td><td>6.4</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Apache Tomcat is prone to multiple remote vulnerabilities including information-disclosure and denial-of-service issues.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.86 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">Remote attackers can exploit these issues to cause denial-of-service conditions or gain access to potentially sensitive information, information obtained may lead to further attacks.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">The vendor released updates. Please see the references for more information.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Apache Tomcat 5.5.0 through 5.5.29, 6.0.0 through 6.0.27, and 7.0.0 beta does not properly handle an invalid Transfer-Encoding header, which allows remote attackers to cause a denial of service (application outage) or obtain sensitive information via a crafted header that interferes with "recycling of a buffer." Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 6.0.24Fixed version 5.5.306.0.287.0.1Installationpath port 8080tcp</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://www.securityfocus.com/bid/41544
http://tomcat.apache.org/security-5.html
http://tomcat.apache.org/security-6.html
http://tomcat.apache.org/security-7.html
http://www.securityfocus.com/archive/1/512272</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2010-3332</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>Windows Microsoft Bulletins</td><td></td><td>CVSS</td><td>6.4</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">This host is missing a critical security update according to Microsoft Bulletin MS10-070.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.9.211 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">Successful exploitation could allow remote attackers to decrypt and gain access to potentially sensitive data encrypted by the server or read data from arbitrary files within an ASP.NET application. Obtained information may aid in further attacks.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">The vendor has released updates. Please see the references for more information.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Microsoft .NET Framework 1.1 SP1, 2.0 SP1 and SP2, 3.5, 3.5 SP1, 3.5.1, and 4.0, as used for ASP.NET in Microsoft Internet Information Services (IIS), provides detailed error codes during decryption attempts, which allows remote attackers to decrypt and modify encrypted View State (aka __VIEWSTATE) form data, and possibly forge cookies or read application files, via a padding oracle attack, aka "ASP.NET Padding Oracle Vulnerability." Microsoft ASP.NET Information Disclosure Vulnerability (2418042)</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://www.vupen.com/english/advisories/2010/2429
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-070
http://www.troyhunt.com/2010/09/fear-uncertainty-and-and-padding-oracle.html
http://weblogs.asp.net/scottgu/archive/2010/09/18/important-asp-net-security-vulnerability.aspx</td></tr>
</table>

CVE-2013-4548							
Risk	High		Threat Type	General		CVSS	6.0
Summary	A memory corruption vulnerability exists in the post-authentication sshd process when an AES-GCM cipher aes128-gcmopenssh.com or aes256-gcmopenssh.com is selected during kex exchange.						
Affected Nodes	192.168.11.76 -						
Impact							
Solution	Update to version 6.4 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	The mm_newkeys_from_blob function in monitor_wrap.c in sshd in OpenSSH 6.2 and 6.3, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address. OpenSSH 6.2 <= 6.3 Permissions, Privileges, and Access Controls Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.2Fixed version 6.4Installationpath port 22tcp						
References	https://www.openssh.com/txt/gcmrekey.adv						

CVE-2013-4286							
Risk	High		Threat Type	Web Servers		CVSS	5.8
Summary	Apache Tomcat is prone to multiple vulnerabilities.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to conduct session fixation attacks and manipulate certain data.						
Solution	Upgrade to version 6.0.39 or 7.0.47 or 8.0.0-RC3 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	Apache Tomcat before 6.0.39, 7.x before 7.0.47, and 8.x before 8.0.0-RC3, when an HTTP connector or AJP connector is used, does not properly handle certain inconsistent HTTP request headers, which allows remote attackers to trigger incorrect identification of a request's length and conduct request-smuggling attacks via (1) multiple Content-Length headers or (2) a Content-Length header and a "Transfer-Encoding: chunked" header. NOTE: this vulnerability exists because of an incomplete fix for CVE-2005-2090. Apache Tomcat Multiple Vulnerabilities - 01 - Mar14						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.397.0.478.0.0-RC3Installationpath port 8080tcp						
References	http://seclists.org/bugtraq/2014/Feb/134 http://packetstormsecurity.com/files/125394						

<table>
<tr><th colspan="8">CVE-2003-1567</th></tr>
<tr><td>Risk</td><td>High</td><td></td><td>Threat Type</td><td>Web Servers</td><td></td><td>CVSS</td><td>5.8</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">The remote web server supports the TRACE andor TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.141 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">An attacker may use this flaw to trick your legitimate web   users to give him their credentials.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Disable the TRACE and TRACK methods in your web server configuration.   Please see the manual of your web server or the references for more information.</td><td colspan="2">Solution Type</td><td>Mitigation</td></tr>
<tr><th colspan="8">Additional Details</th></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">The undocumented TRACK method in Microsoft Internet Information Services (IIS) 5.0 returns the content of the original request in the body of the response, which makes it easier for remote attackers to steal cookies and authentication credentials, or bypass the HttpOnly protection mechanism, by using TRACK to read the contents of the HTTP headers that are returned in the response, a technique that is similar to cross-site tracing (XST) using HTTP TRACE. HTTP Debugging Methods (TRACE/TRACK) Enabled</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if HTTP methods such as TRACE and TRACK are   enabled and can be used.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">The web server has the following HTTP methods enabled TRACE</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://www.kb.cert.org/vuls/id/288308
http://www.kb.cert.org/vuls/id/867593
https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trace-verbs/ba-p/784482
https://owasp.org/www-community/attacks/Cross_Site_Tracing</td></tr>
</table>

CVE-2014-0224							
Risk	**High**		**Threat Type**	SSL and TLS		**CVSS**	**5.8**
Summary	OpenSSL is prone to security-bypass vulnerability.						
Affected Nodes	192.168.3.184 -						
Impact	Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.						
Solution	Updates are available. Please see the references for more information.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability. SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability						
Detection Method	Send two SSL ChangeCipherSpec request and check the response.						
References	https://www.openssl.org/news/secadv/20140605.txt http://www.securityfocus.com/bid/67899						

CVE-2014-2532							
Risk	**High**		**Threat Type**	General		**CVSS**	**5.8**
Summary	OpenSSH is prone to a security-bypass vulnerability.						
Affected Nodes	192.168.11.76 -						
Impact	The security bypass allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.						
Solution	Updates are available. Please see the references for more information.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character. OpenSSH 'child_set_env()' Function Security Bypass Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.2Fixed version 6.6Installationpath port 22tcp						
References	http://www.securityfocus.com/bid/66355						

CVE-2019-18677							
Risk	High		Threat Type	Web application abuses		CVSS	5.8
Summary	Squid is prone to multiple vulnerabilities.						
Affected Nodes	192.168.1.251 -						
Solution	Update to version 4.9 or later.				Solution Type	VendorFix	
Additional Details							
CVE Description	An issue was discovered in Squid 2.x, 3.x, and 4.x through 4.8. Due to incorrect data management, it is vulnerable to information disclosure when processing HTTP Digest Authentication. Nonce tokens contain the raw byte value of a pointer that sits within heap memory allocation. This information reduces ASLR protections and may aid attackers isolating memory areas to target for remote code execution attacks. Squid Proxy Cache Multiple Security Update Advisories (SQUID-2019:9, SQUID-2019:11)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.9						
References	http://www.squid-cache.org/Advisories/SQUID-2019_9.txt http://www.squid-cache.org/Advisories/SQUID-2019_11.txt						

CVE-2014-2653							
Risk	High		Threat Type	General		CVSS	5.8
Summary	OpenSSH is prone to a security-bypass vulnerability.						
Affected Nodes	192.168.11.76 -						
Impact	Attackers can exploit this issue to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.						
Solution	Updates are available. Please see the references for more information.				Solution Type	VendorFix	
Additional Details							
CVE Description	The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate. OpenSSH Certificate Validation Security Bypass Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.2Fixed version See referencesInstallationpath port 22tcp						
References	http://www.securityfocus.com/bid/66459						

CVE-2018-20685							
Risk	High		**Threat Type**	General		**CVSS**	5.8
Summary	OpenBSD OpenSSH is prone to multiple vulnerabilities.						
Affected Nodes	192.168.11.14 -						
Solution	Update to version 8.0 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file). OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version 8.0Installationpath port 22tcp						
References	https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt http://www.openwall.com/lists/oss-security/2019/04/18/1						

CVE-2016-3115							
Risk	High		**Threat Type**	General		**CVSS**	5.5
Summary	openssh xauth command injection may lead to forced-command and binfalse bypass						
Affected Nodes	192.168.11.14 -						
Impact	By injecting xauth commands one gains limited* read/write arbitrary files, information leakage or xauth-connect capabilities.						
Solution	Upgrade to OpenSSH version 7.2p2 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions. OpenSSH <= 7.2p1 - Xauth Injection						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version 7.2p2Installationpath port 22tcp						
References	http://www.openssh.com/txt/release-7.2p2						

CVE-2016-3116							
Risk	High		**Threat Type**	General		**CVSS**	5.5
Summary	Dropbear SSH is prone to a CRLF injection vulnerability.						
Affected Nodes	192.168.11.22 -						
Impact	Successfully exploiting this issue allow remote authenticated users to inject commands to xauth.						
Solution	Update to Dropbear SSH version 2016.72 or later.				**Solution Type**		VendorFix
Additional Details							
CVE Description	CRLF injection vulnerability in Dropbear SSH before 2016.72 allows remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data. Dropbear SSH < 2016.72 CRLF Injection Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 2015.68Fixed version 2016.72Installationpath port 2400tcp						
References	https://matt.ucc.asn.au/dropbear/CHANGES https://github.com/tintinweb/pub/tree/master/pocs/cve-2016-3116						

CVE-2016-5388							
Risk	High		Threat Type	Web Servers		CVSS	5.1
Summary	Apache Tomcat is prone to a man-in-the-middle MITM vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to conduct MITM attacks on internal server subrequests or direct the server to initiate connections to arbitrary hosts.						
Solution	Information is available and linked in the references about a configuration or deployment scenario that helps to reduce the risk of the vulnerability.				Solution Type	Mitigation	
Additional Details							
CVE Description	Apache Tomcat 7.x through 7.0.70 and 8.x through 8.5.4, when the CGI Servlet is enabled, follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "A mitigation is planned for future releases of Tomcat, tracked as CVE-2016-5388"; in other words, this is not a CVE ID for a vulnerability. Apache Tomcat 'CGI Servlet' MITM Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version MitigationInstallationpath port 8080tcp						
References	http://www.kb.cert.org/vuls/id/BLUU-ABSLHW http://www.securityfocus.com/bid/91818 https://www.apache.org/security/asf-httpoxy-response.txt						

Medium Risk (123)

A Medium Risk Vulnerability will cause disruptions to a network and create the potential for network/data breaches. An attack successfully carried out on these vulnerabilities will affect systems and associated programs. These vulnerabilities might also allow attackers to access critical data.

CVE-2002-0876							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary	It was possible to kill the web server by sending a malicious request.						
Affected Nodes	192.168.60.53 -						
Solution	Install a safer server or upgrade it.				**Solution Type**		VendorFix
Additional Details							
CVE Description	Web server for Shambala 4.5 allows remote attackers to cause a denial of service (crash) via a malformed HTTP request. Shambala web server DoS						

CVE-2003-0180							
Risk	**Medium**		**Threat Type**	Gain a shell remotely		**CVSS**	**5.0**
Summary	It was possible to kill the web server by sending an invalid request with a too long HTTP 1.1 header Accept-Encoding Accept-Language Accept-Range Connection Expect If-Match If-None-Match If-Range If-Unmodified-Since Max-Forwards TE Host						
Affected Nodes	192.168.11.73 -						
Impact	An attacker may exploit this vulnerability to make the web server crash continually or even execute arbitrtay code on your system.						
Solution	Upgrade your software or protect it with a filtering reverse proxy.				**Solution Type**		VendorFix
Additional Details							
CVE Description	Lotus Domino Web Server (nhttp.exe) before 6.0.1 allows remote attackers to cause a denial of service via an incomplete POST request, as demonstrated using the h_PageUI form. HTTP 1.1 header overflow						

CVE-2018-1000027							
Risk	**Medium**		**Threat Type**	Web application abuses		**CVSS**	**5.0**
Summary	Squid is vulnerable to denial of service attack when processing ESI responses.						
Affected Nodes	192.168.1.251 -						
Impact	This problem allows a remote server delivering certain ESI response syntax to trigger a denial of service for all clients accessing the Squid service.						
Solution	Updated Packages: This bug is fixed by Squid version 4.0.23. In addition, patches addressing this problem for the stable releases can be found in our patch archives for Squid 3.5 and Squid 4. If you are using a prepackaged version of Squid then please refer to the package vendor for availability information on updated packages.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The Squid Software Foundation Squid HTTP Caching Proxy version prior to version 4.0.23 contains a NULL Pointer Dereference vulnerability in HTTP Response X-Forwarded-For header processing that can result in Denial of Service to all clients of the proxy. This attack appear to be exploitable via Remote HTTP server responding with an X-Forwarded-For header to certain types of HTTP request. This vulnerability appears to have been fixed in 4.0.23 and later. Squid Proxy Cache Security Update Advisory SQUID-2018:2						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version See references						
References	http://www.squid-cache.org/Advisories/SQUID-2018_2.txt http://www.squid-cache.org/Versions/v3/3.5/changesets/SQUID-2018_2.patch http://www.squid-cache.org/Versions/v4/changesets/SQUID-2018_2.patch						

CVE-2018-1000024							
Risk	**Medium**		**Threat Type**	Web application abuses		**CVSS**	**5.0**
Summary	Squid is vulnerable to denial of service attack when processing ESI responses.						
Affected Nodes	192.168.1.251 -						
Impact	This problem allows a remote server delivering certain ESI response syntax to trigger a denial of service for all clients accessing the Squid service.						
Solution	Upgrade to 4.0.23 or later. Patches are available, please see the references for details.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	The Squid Software Foundation Squid HTTP Caching Proxy version 3.0 to 3.5.27, 4.0 to 4.0.22 contains a Incorrect Pointer Handling vulnerability in ESI Response Processing that can result in Denial of Service for all clients using the proxy.. This attack appear to be exploitable via Remote server delivers an HTTP response payload containing valid but unusual ESI syntax.. This vulnerability appears to have been fixed in 4.0.23 and later. Squid Proxy Cache Security Update Advisory SQUID-2018:1						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.0.23						
References	http://www.squid-cache.org/Advisories/SQUID-2018_1.txt						

<table>
<tr><th colspan="8">CVE-2016-10003</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>Web application abuses</td><td></td><td><b>CVSS</b></td><td><b>5.0</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">Squid is prone an information disclosure vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.1.251 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6">This problem allows a remote attacker to discover private and sensitive information about another clients browsing session. Potentially including credentials which allow access to further sensitive resources. This problem only affects Squid configured to use the Collapsed Forwarding feature.</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">Upgrade to 3.5.23, 4.0.17 or later.</td><td colspan="2"><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">Incorrect HTTP Request header comparison in Squid HTTP Proxy 3.5.0.1 through 3.5.22, and 4.0.1 through 4.0.16 results in Collapsed Forwarding feature mistakenly identifying some private responses as being suitable for delivery to multiple clients. Squid Information Disclosure Vulnerability (Linux)</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 3.5.20Fixed version   3.5.23</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">http://www.squid-cache.org/Advisories/SQUID-2016_10.txt</td></tr>
</table>

CVE-2016-10002							
Risk	Medium		Threat Type	Web application abuses		CVSS	5.0
Summary	Squid is prone an information disclosure vulnerability.						
Affected Nodes	192.168.1.251 -						
Impact	A remote attacker may discover private and sensitive information about another clients browsing session. Potentially including credentials which allow access to further sensitive resources.						
Solution	Upgrade to 3.5.23, 4.0.17 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	Incorrect processing of responses to If-None-Modified HTTP conditional requests in Squid HTTP Proxy 3.1.10 through 3.1.23, 3.2.0.3 through 3.5.22, and 4.0.1 through 4.0.16 leads to client-specific Cookie data being leaked to other clients. Attack requests can easily be crafted by a client to probe a cache for this information. Squid Information Disclosure Vulnerability (Linux)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 3.5.23						
References	http://www.squid-cache.org/Advisories/SQUID-2016_11.txt						

CVE-2020-25097							
Risk	Medium		Threat Type	Web application abuses		CVSS	5.0
Summary	Squid is prone to an HTTP request smuggling vulnerability.						
Affected Nodes	192.168.1.251 -						
Impact							
Solution	Update to version 4.13, 5.0.5 or later. See the referenced vendor advisory for a workaround.					Solution Type	VendorFix
Additional Details							
CVE Description	An issue was discovered in Squid through 4.13 and 5.x through 5.0.4. Due to improper input validation, it allows a trusted client to perform HTTP Request Smuggling and access services otherwise forbidden by the security controls. This occurs for certain uri_whitespace configuration settings. Squid 2.0 < 4.14, 5.0.1 < 5.0.5 HTTP Request Smuggling Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.14Installationpath port 3128tcp						
References	https://github.com/squid-cache/squid/security/advisories/GHSA-jvf6-h9gj-pmj6						

CVE-2020-14058							
Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	Squid is prone to a denial of service vulnerability in the TLS handshake.						
Affected Nodes	192.168.1.251 -						
Solution	Update to version 4.12, 5.0.3 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	An issue was discovered in Squid before 4.12 and 5.x before 5.0.3. Due to use of a potentially dangerous function, Squid and the default certificate validation helper are vulnerable to a Denial of Service when opening a TLS connection to an attacker-controlled server for HTTPS. This occurs because unrecognized error values are mapped to NULL, but later code expects that each error value is mapped to a valid error string. Squid Proxy Cache Security Update Advisory SQUID-2020:6						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.12						
References	http://www.squid-cache.org/Advisories/SQUID-2020_6.txt						

CVE-2021-28651							
Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	Squid is prone to a denial of service DoS vulnerability in the URN processing.						
Affected Nodes	192.168.1.251 -						
Solution	Update to version 4.15, 5.0.6 or later. See the referenced vendor advisory for a workaround.					Solution Type	VendorFix
Additional Details							
CVE Description	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. Due to a buffer-management bug, it allows a denial of service. When resolving a request with the urn: scheme, the parser leaks a small amount of memory. However, there is an unspecified attack methodology that can easily trigger a large amount of memory consumption. Squid 2.0 < 4.14, 5.0.1 < 5.0.5 DoS Vulnerability (SQUID-2021:1)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.15Installationpath port 3128tcp						
References	https://github.com/squid-cache/squid/security/advisories/GHSA-ch36-9jhx-phm4						

CVE-2000-0182							
Risk	**Medium**		**Threat Type**	Gain a shell remotely		**CVSS**	**5.0**
Summary	It was possible to kill the web server by sending an invalid request with a too long header name or value.						
Affected Nodes	192.168.11.73 -						
Impact	An attacker cracker may exploit this vulnerability to make your web server crash continually or even execute arbitrary code on your system.						
Solution	Upgrade your software or protect it with a filtering reverse proxy.					**Solution Type**	VendorFix
Additional Details							
CVE Description	IPlanet Web Server 4.1 allows remote attackers to cause a denial of service via a large number of GET commands, which consumes memory and causes a kernel panic. HTTP header overflow						

CVE-2014-7810							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Apache Tomcat is prone to a security bypass vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to bypass certain authentication and obtain sensitive information.						
Solution	Upgrade to version 6.0.44 or 7.0.58 or 8.0.16 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The Expression Language (EL) implementation in Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.58, and 8.x before 8.0.16 does not properly consider the possibility of an accessible interface implemented by an inaccessible class, which allows attackers to bypass a SecurityManager protection mechanism via a web application that leverages use of incorrect privileges during EL evaluation. Apache Tomcat SecurityManager Security Bypass Vulnerability - Jun15 (Windows)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.44Installationpath port 8080tcp						
References	http://tomcat.apache.org/security-6.html http://www.securityfocus.com/bid/74665 http://tomcat.apache.org/security-7.html						

<table>
<tr><th colspan="8">CVE-2001-0649</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>Denial of Service</td><td></td><td>CVSS</td><td>5.0</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">It was possible to kill the Personal Web Sharing service by sending it a too long request.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.1.103 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">An attacker may exploit this vulnerability to make your web server   crash continually.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Upgrade your software or protect it with a filtering reverse proxy.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Personal Web Sharing 1.5.5 allows a remote attacker to cause a denial of service via a long HTTP request. Personal Web Sharing overflow</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2016-6794</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>Web Servers</td><td></td><td>CVSS</td><td>5.0</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Apache Tomcat is prone to security bypass and information disclosure vulnerabilities.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.86 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">Successful exploitation will allow remote   attackers to gain access to potentially sensitive information and bypass   certain security restrictions.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Upgrade to Apache Tomcat version 9.0.0.M10   or 8.5.5 or 8.0.37 or 7.0.72 or 6.0.47 or later.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">When a SecurityManager is configured, a web application's ability to read system properties should be controlled by the SecurityManager. In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70, 6.0.0 to 6.0.45 the system property replacement feature for configuration files could be used by a malicious web application to bypass the SecurityManager and read system properties that should not be visible. Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities (Windows)</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 6.0.24Fixed version   6.0.47Installationpath port   8080tcp</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.72
http://www.securityfocus.com/bid/93940
http://www.securityfocus.com/bid/93944
http://www.securityfocus.com/bid/93939
http://www.securityfocus.com/bid/93942
http://www.securityfocus.com/bid/93943
http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.47
http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M10
http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.5_and_8.0.37</td></tr>
</table>

CVE-2016-8745							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Apache Tomcat is prone to an information disclosure vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to gain access to potentially sensitive information.						
Solution	Upgrade to Apache Tomcat version 9.0.0.M15 or 8.5.9 or 8.0.41 or 7.0.75 or 6.0.50 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	A bug in the error handling of the send file code for the NIO HTTP connector in Apache Tomcat 9.0.0.M1 to 9.0.0.M13, 8.5.0 to 8.5.8, 8.0.0.RC1 to 8.0.39, 7.0.0 to 7.0.73 and 6.0.16 to 6.0.48 resulted in the current Processor object being added to the Processor cache multiple times. This in turn meant that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body. The bug was first noticed in 8.5.x onwards where it appears the refactoring of the Connector code for 8.5.x onwards made it more likely that the bug was observed. Initially it was thought that the 8.5.x refactoring introduced the bug but further investigation has shown that the bug is present in all currently supported Tomcat versions. Apache Tomcat NIO HTTP connector Information Disclosure Vulnerability (Windows)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.50Installationpath port 8080tcp						
References	https://bz.apache.org/bugzilla/show_bug.cgi?id=60409 http://www.securityfocus.com/bid/94828 http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M15 http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.41 http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.75 http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.9 http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.50						

<table>
<tr><th colspan="8">CVE-2014-0075</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>Web Servers</td><td></td><td>CVSS</td><td>5.0</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Apache Tomcat is prone to multiple vulnerabilities.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.86 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">Successful exploitation will allow remote attackers to cause a   denial of service (resource consumption), bypass security-manager restrictions and read arbitrary files, conducted by HTTP request smuggling attacks via a crafted Content-Length HTTP header.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Update to version 6.0.40, 7.0.53, 8.0.4 or later.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Java/org/apache/catalina/servlets/DefaultServlet.java in the default servlet in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 does not properly restrict XSLT stylesheets, which allows remote attackers to bypass security-manager restrictions and read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. Apache Tomcat Multiple Vulnerabilities (Nov 2014)</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 6.0.24Fixed version   6.0.407.0.538.0.4Installationpath port 8080tcp</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://secunia.com/advisories/60729
http://tomcat.apache.org/security-8.html
http://tomcat.apache.org/security-7.html
http://tomcat.apache.org/security-6.html</td></tr>
</table>

CVE-2011-1184							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Apache Tomcat Server is prone to multiple security bypass vulnerabilities.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation could allows remote attackers to bypass intended access restrictions or gain sensitive information.						
Solution	Upgrade Apache Tomcat to 5.5.34, 6.0.33, 7.0.12 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not have the expected countermeasures against replay attacks, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, related to lack of checking of nonce (aka server nonce) and nc (aka nonce-count or client nonce count) values. Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows)						
Findings	Installed version 6.0.24Fixed version 5.5.346.0.337.0.12Installationpath port 8080tcp						
References	http://tomcat.apache.org/security-5.html http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-7.html http://svn.apache.org/viewvc?view=revision&revision=1158180 http://svn.apache.org/viewvc?view=revision&revision=1159309 http://svn.apache.org/viewvc?view=revision&revision=1087655						

CVE-2012-5887							
Risk	Medium		Threat Type	Web Servers		CVSS	5.0
Summary	Apache Tomcat Server is prone to multiple security bypass vulnerabilities.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation could allow remote attackers to bypass intended access restrictions by sniffing the network for valid requests.						
Solution	Apply patch or upgrade Apache Tomcat to 5.5.36, 6.0.36, 7.0.30 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	The replay-countermeasure functionality in the HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 tracks cnonce (aka client nonce) values instead of nonce (aka server nonce) and nc (aka nonce-count) values, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, a different vulnerability than CVE-2011-1184. Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows)						
Findings	Installed version 6.0.24Fixed version 5.5.366.0.367.0.30Installationpath port 8080tcp						
References	http://secunia.com/advisories/51138/ http://tomcat.apache.org/security-5.html#Fixed_in_Apache_Tomcat_5.5.36 http://tomcat.apache.org/security-6.html#Fixed_in_Apache_Tomcat_6.0.36 http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.30 http://svn.apache.org/viewvc?view=revision&revision=1377807 http://svn.apache.org/viewvc?view=revision&revision=1380829 http://svn.apache.org/viewvc?view=revision&revision=1392248						

CVE-2011-4858							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Apache Tomcat Server is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation could allow remote attackers to cause a denial of service via a specially crafted form sent in a HTTP POST request.						
Solution	Apply patch or upgrade Apache Tomcat to 5.5.35, 6.0.35, 7.0.23 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Apache Tomcat before 5.5.35, 6.x before 6.0.35, and 7.x before 7.0.23 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters. Apache Tomcat Hash Collision Denial Of Service Vulnerability						
Findings	Installed version 6.0.24Fixed version 5.5.356.0.357.0.23Installationpath port 8080tcp						
References	http://www.kb.cert.org/vuls/id/903934 https://bugzilla.redhat.com/show_bug.cgi?id=750521 http://www.ocert.org/advisories/ocert-2011-003.html http://tomcat.apache.org/tomcat-7.0-doc/changelog.html						

CVE-2012-2733							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Apache Tomcat Server is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation could allow remote attackers to cause a denial of service condition.						
Solution	Apply patch or upgrade Apache Tomcat to 6.0.36, 7.0.28 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Java/org/apache/coyote/http11/InternalNioInputBuffer.java in the HTTP NIO connector in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.28 does not properly restrict the request-header size, which allows remote attackers to cause a denial of service (memory consumption) via a large amount of header data. Apache Tomcat HTTP NIO Denial Of Service Vulnerability (Windows)						
Findings	Installed version 6.0.24Fixed version 6.0.367.0.28Installationpath port 8080tcp						
References	http://secunia.com/advisories/51138 http://svn.apache.org/viewvc?view=revision&revision=1350301 http://svn.apache.org/viewvc?view=revision&revision=1356208 http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-7.html						

CVE-2015-5345							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Apache Tomcat is prone to Directory Disclosure Vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation allows remote attackers to determine the existence of a directory.						
Solution	Upgrade to version 6.0.45 or 7.0.67 or 8.0.30 or 9.0.0.M3 later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The Mapper component in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.30, and 9.x before 9.0.0.M2 processes redirects before considering security constraints and Filters, which allows remote attackers to determine the existence of a directory via a URL that lacks a trailing / (slash) character. Apache Tomcat Directory Disclosure Vulnerability - Feb16 (Windows)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.45Installationpath port 8080tcp						
References	http://tomcat.apache.org/security-9.html http://www.securityfocus.com/bid/83328 http://tomcat.apache.org/security-8.html http://tomcat.apache.org/security-7.html http://tomcat.apache.org/security-6.html https://bz.apache.org/bugzilla/show_bug.cgi?id=58765						

Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary	The remote SMC 2652W Access point web server crashes when sent a specially formatted HTTP request.						
Affected Nodes	192.168.1.103 -						
Solution	Contact vendor for a fix.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Crash SMC AP						

CVE-2002-1663							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary	Your web server crashes when it receives an incorrect POST command with an empty Content-Length field.						
Affected Nodes	192.168.1.103 -						
Impact	An attacker may use this bug to disable your server, preventing it from publishing your information.						
Solution	Upgrade your web server.				**Solution Type**		VendorFix
Additional Details							
CVE Description	The Post_Method function in method.c for Monkey HTTP Daemon before 0.5.1 allows remote attackers to cause a denial of service (crash) via a POST request with an invalid or missing Content-Length header value. POST with empty Content-Length						

CVE-2017-5647							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Apache Tomcat is prone to an information disclosure vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to obtain sensitive information from requests other then their own.						
Solution	Upgrade to version 9.0.0.M19, 8.5.13, 8.0.43, 7.0.77, 6.0.53 or later.				**Solution Type**		VendorFix
Additional Details							
CVE Description	A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C. Apache Tomcat 'pipelined' Requests Information Disclosure Vulnerability (Windows)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.53Installationpath port 8080tcp						
References	http://tomcat.apache.org/security-9.html http://tomcat.apache.org/security-8.html http://tomcat.apache.org/security-7.html http://tomcat.apache.org/security-6.html https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0dee9190ba48171451a@%3Cusers.tomcat.apache.org%3E						

Risk	**Medium**		**Threat Type**	Web application abuses		**CVSS**	**5.0**
Summary	The script reports backup files left on the web server. Notes - Unreliable Detection means that a file was detected only based on a HTTP 200 Found status code reported by the remote web server when a file was requested. - As the VT Backup File Scanner HTTP OID 1.3.6.1.4.1.25623.1.0.140853 might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.						
Affected Nodes	192.168.11.76 -						
Impact	Based on the information provided in this files an attacker might be able to gather sensitive information stored in these files.						
Solution	Delete the backup files.				**Solution Type**	Mitigation	
Additional Details							
CVE Description	Backup File Scanner (HTTP) - Unreliable Detection Reporting						
Detection Method	Reports previous enumerated backup files accessible on the remote web server.						
Findings	The following backup files were identified URLMatching patternhttp192.168.11.76downloadsEventideMediaAgentDesktopInstaller2.8.6639.exeHTTP1.01 200http192.168.11.76downloadsEventideMediaWorksPlusDesktopInstaller2.8.6639.exeHTTP1.01 200						
References	http://www.openwall.com/lists/oss-security/2017/10/31/1						

<table>
<tr><th colspan="8">CVE-2016-1409</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>CISCO</td><td></td><td>CVSS</td><td>5.0</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">A vulnerability in the IP Version 6 IPv6 packet processing functions of Cisco IOS XR Software Cisco IOS Software Cisco IOS XE Software and Cisco NX-OS Software could allow an unauthenticated remote attacker to cause an affected device to stop processing IPv6 traffic leading to a denial of service DoS condition on the device. The vulnerability is due to insufficient processing logic for crafted IPv6 packets that are sent to an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 Neighbor Discovery packets to an affected device for processing. A successful exploit could allow the attacker to cause the device to stop processing IPv6 traffic leading to a DoS condition on the device. Cisco will release software updates that address this vulnerability. There are no workarounds that address this vulnerability.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.30.254 -</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">See the referenced vendor advisory for a solution.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">The Neighbor Discovery (ND) protocol implementation in the IPv6 stack in Cisco IOS XE 2.1 through 3.17S, IOS XR 2.0.0 through 5.3.2, and NX-OS allows remote attackers to cause a denial of service (packet-processing outage) via crafted ND messages, aka Bug ID CSCuz66542, as exploited in the wild in May 2016. Cisco Products IPv6 Neighbor Discovery Crafted Packet Denial of Service Vulnerability</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 12.415XZFixed version   See advisory</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160525-ipv6</td></tr>
</table>

CVE-2016-6415							
Risk	**Medium**		**Threat Type**	CISCO		**CVSS**	**5.0**
Summary	A vulnerability in IKEv1 packet processing code in Cisco IOS Softwarecould allow an unauthenticated remote attacker to retrieve memory contents which could lead to thedisclosure of confidential information.						
Affected Nodes	192.168.30.254 -						
Impact	A successful exploit could allow the attacker to retrieve memory contents, which could lead to the disclosure of confidential information.						
Solution	The vendor has released updates, please see the referenced vendor advisory for more information on the fixed versions.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The server IKEv1 implementation in Cisco IOS 12.2 through 12.4 and 15.0 through 15.6, IOS XE through 3.18S, IOS XR 4.3.x and 5.0.x through 5.2.x, and PIX before 7.0 allows remote attackers to obtain sensitive information from device memory via a Security Association (SA) negotiation request, aka Bug IDs CSCvb29204 and CSCvb36055 or BENIGNCERTAIN. Cisco IOS Software IKEv1 Information Disclosure Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 12.415XZFixed version See advisory						
References	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1 https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvb29204 https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvb36055						

CVE-1999-1196							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary	It was possible to crash the remote service by sending it a few kilobytes of random data.						
Affected Nodes	192.168.20.58 -						
Impact	An attacker may use this flaw to make this service crash continuously, preventing this service from working properly. It may also be possible to exploit this flaw to execute arbitrary code on this host.						
Solution	Upgrade your software or contact your vendor and inform it of this vulnerability.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Hummingbird Exceed X version 5 allows remote attackers to cause a denial of service via malformed data to port 6000. Kill service with random data						

CVE-2021-28169							
Risk	**Medium**		**Threat Type**	Web application abuses		**CVSS**	**5.0**
Summary	Eclipse Jetty is prone to an information disclosure vulnerability in the ConcatServlet and WelcomeFilter servlet.						
Affected Nodes	192.168.11.226 -						
Impact							
Solution	Update to version 9.4.41, 10.0.3, 11.0.3 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	For Eclipse Jetty versions &amp;lt;= 9.4.40, &amp;lt;= 10.0.2, &amp;lt;= 11.0.2, it is possible for requests to the ConcatServlet with a doubly encoded path to access protected resources within the WEB-INF directory. For example a request to `/concat?/%2557EB-INF/web.xml` can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application. Eclipse Jetty Information Disclosure Vulnerability (GHSA-gwcr-j4wh-j3cq)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 7.6.9.20130131Fixed version 9.4.41Installationpath port 6143tcp						
References	https://github.com/eclipse/jetty.project/security/advisories/GHSA-gwcr-j4wh-j3cq						

CVE-2019-10247							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Eclypse Jetty is prone to an information disclosure vulnerability.						
Affected Nodes	192.168.11.226 -						
Solution	Update to version 9.2.28.v20190418, 9.3.27.v20190418, 9.4.17.v20190418 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	In Eclipse Jetty version 7.x, 8.x, 9.2.27 and older, 9.3.26 and older, and 9.4.16 and older, the server running on any OS and Jetty version combination will reveal the configured fully qualified directory base resource location on the output of the 404 error for not finding a Context that matches the requested path. The default server behavior on jetty-distribution and jetty-home will include at the end of the Handler tree a DefaultHandler, which is responsible for reporting this 404 error, it presents the various configured contexts as HTML for users to click through to. This produced HTML includes output that contains the configured fully qualified directory base resource location for each context. Eclipse Jetty Information Disclosure Vulnerability - CVE-2019-10247 (Windows)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 7.6.9.20130131Fixed version 9.2.28.20190418Installationpath port 6143tcp						
References	https://bugs.eclipse.org/bugs/show_bug.cgi?id=546577 https://github.com/eclipse/jetty.project/issues/3555						

Risk	**Medium**		**Threat Type**	Web application abuses		**CVSS**	**5.0**
Summary	The printenv CGI is installed. printenv normally returns all environment variables.						
Affected Nodes	192.168.192.168 -						
Impact	This gives an attacker valuable information about the configuration of your web server.						
Solution	Remove it from /cgi-bin.					**Solution Type**	Workaround
Additional Details							
CVE Description	printenv						
Findings	Vulnerable URL http192.168.192.168webuiprintenv						

CVE-2012-3505							
Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	Tinyproxy is prone to multiple remote denial-of-service vulnerabilities that affect the OpenSSL extension.						
Affected Nodes	192.168.13.48 -						
Impact	Successful attacks will cause the application to consume excessive memory, creating a denial-of-service condition.						
Solution	Upgrade to Tinyproxy 1.8.4.				Solution Type		VendorFix
Additional Details							
CVE Description	Tinyproxy 1.8.3 and earlier allows remote attackers to cause a denial of service (CPU and memory consumption) via (1) a large number of headers or (2) a large number of forged headers that trigger hash collisions predictably. bucket. Tinyproxy < 1.8.4 Header Multiple Denial of Service Vulnerabilities						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.8.2Fixed version 1.8.4						
References	http://www.securityfocus.com/bid/55099						

CVE-2009-4496							
Risk	Medium		Threat Type	Web Servers		CVSS	5.0
Summary	Boa Webserver is prone to a command-injection vulnerability because it fails to adequately sanitize user-supplied input in logfiles.						
Affected Nodes	192.168.9.117 -						
Impact	Attackers can exploit this issue to execute arbitrary commands in a terminal.						
Solution	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.				Solution Type		WillNotFix
Additional Details							
CVE Description	Boa 0.94.14rc21 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator. Boa Webserver Terminal Escape Sequence in Logs Command Injection Vulnerability						
References	http://www.securityfocus.com/bid/37718 http://www.securityfocus.com/archive/1/508830						

Risk	**Medium**		**Threat Type**	SMTP problems		**CVSS**	**5.0**
Summary		The Mailserver on this host answers to VRFY andor EXPN requests.					
Affected Nodes		192.168.11.216 -					
Impact							
Solution		Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.				**Solution Type**	Workaround
Additional Details							
CVE Description		Check if Mailserver answer to VRFY and EXPN requests					
Findings		VRFY root produces the following answer 252 2.0.0 root					
References		http://cr.yp.to/smtp/vrfy.html					

CVE-2002-1906							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary		The remote web server locks up when several incomplete web requests are sent and the connections are kept open.					
Affected Nodes		192.168.1.103 -					
Solution		Contact your vendor for a patch, upgrade your web server.				**Solution Type**	VendorFix
Additional Details							
CVE Description		The web server for Polycom ViaVideo 2.2 and 3.0 allows remote attackers to cause a denial of service (CPU consumption) by sending incomplete HTTP requests and leaving the connections open. Polycom ViaVideo denial of service					
Detection Method							
Findings							
References							

Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	It was possible to kill the remote web server by requesting something like This is probably a Compaq Web Enterprise Management server.						
Affected Nodes	192.168.3.253 -						
Impact	An attacker might use this flaw to forbid you from managing your machines.						
Solution	contact your vendor for a patch, or disable this service if you do not use it.					Solution Type	VendorFix
Additional Details							
CVE Description	Compaq Web SSI DoS						

CVE-2012-5533							
Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	Lighttpd HTTP Server is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.3.253 -						
Impact	Successful exploitation could allow attackers to cause a denial of service via crafted Connection header values.						
Solution	Upgrade to 1.4.32 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	The http_request_split_value function in request.c in lighttpd before 1.4.32 allows remote attackers to cause a denial of service (infinite loop) via a request with a header containing an empty token, as demonstrated using the "Connection: TE,,Keep-Alive" header. Lighttpd Connection header Denial of Service Vulnerability						
References	http://seclists.org/oss-sec/2012/q4/320 http://www.exploit-db.com/exploits/22902 http://www.lighttpd.net/2012/11/21/1-4-32 http://seclists.org/fulldisclosure/2012/Nov/156 http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2012_01.txt						

CVE-2002-1052							
Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	It was possible to crash the Jigsaw web server by requesting servletcon about 30 times.						
Affected Nodes	192.168.3.193 -						
Impact	An attacker may use this attack to make this service crash continuously.						
Solution	Upgrade your software.					Solution Type	VendorFix
Additional Details							
CVE Description	Jigsaw 2.2.1 on Windows systems allows remote attackers to use MS-DOS device names in HTTP requests to (1) cause a denial of service using the "con" device, or (2) obtain the physical path of the server using two requests to the "aux" device. Jigsaw webserver MS/DOS device DoS						

Risk	Medium		Threat Type	Web application abuses		CVSS	5.0
Summary	The application is missing the httpOnly cookie attribute						
Affected Nodes	192.168.3.254 -						
Impact							
Solution	Set the 'httpOnly' attribute for any session cookie.					Solution Type	Mitigation
Additional Details							
CVE Description	Missing `httpOnly` Cookie Attribute						
Detection Method	Check all cookies sent by the application for a missing 'httpOnly' attribute						
Findings	The cookiesSet-Cookie AIROSSESSIONIDreplaced Path Version1are missing the httpOnly attribute.						
References	https://www.owasp.org/index.php/HttpOnly https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)						

CVE-2002-2370							
Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	We could crash the remote web server by sending an unfinished line. without a return carriage at the end of the line.						
Affected Nodes	192.168.3.193 -						
Impact	An attacker cracker may exploit this flaw to disable this service.						
Solution	Upgrade your web server.				Solution Type		VendorFix
Additional Details							
CVE Description	SWS web server 0.0.4, 0.0.3 and 0.1.0 allows remote attackers to cause a denial of service (crash) via a URL request that does not end with a newline. HTTP unfinished line denial						

CVE-2002-1236							
Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	The Linksys BEFSR41 EtherFast CableDSL Router crashes if somebody accesses the Gozila CGI without argument on the web administration interface.						
Affected Nodes	192.168.3.187 -						
Solution	Upgrade your router firmware to 1.42.7.				Solution Type		VendorFix
Additional Details							
CVE Description	The remote management web server for Linksys BEFSR41 EtherFast Cable/DSL Router before firmware 1.42.7 allows remote attackers to cause a denial of service (crash) via an HTTP request to Gozila.cgi without any arguments. Linksys Gozila CGI denial of service						

Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary	The remote host answers to TCP packets that are coming from a multicast address. This is known as the spank denial of service attack.						
Affected Nodes	192.168.3.22 -						
Impact	An attacker might use this flaw to shut down this server and saturate your network, thus preventing you from working properly. This also could be used to run stealth scans against your machine.						
Solution	Contact your operating system vendor for a patch. Filter out multicast addresses (224.0.0.0/4).				**Solution Type**	Mitigation	
Additional Details							
CVE Description	'spank' Denial of Service Vulnerability						
Findings	The remote host crashed when it received a TCP packet that were coming from a multicast address. This is known as the spank denial of service attack.						

CVE-2002-1169							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary	We could crash the WebSphere Edge caching proxy by sending a bad request to the helpout.exe CGI						
Affected Nodes	192.168.1.103 -						
Solution	Upgrade your web server or remove this CGI.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	IBM Web Traffic Express Caching Proxy Server 3.6 and 4.x before 4.0.1.26 allows remote attackers to cause a denial of service (crash) via an HTTP request to helpout.exe with a missing HTTP version number, which causes ibmproxy.exe to crash. WebSphere Edge caching proxy denial of service						
Findings	Vulnerable URL http192.168.1.1039295.cobalthelpout.exe						

CVE-2012-3544							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Apache Tomcat Server is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation could allow remote attackers to cause a denial of service via a specially crafted request.						
Solution	Apply patch or upgrade Apache Tomcat to 7.0.30 or 6.0.38 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Apache Tomcat 6.x before 6.0.37 and 7.x before 7.0.30 does not properly handle chunk extensions in chunked transfer coding, which allows remote attackers to cause a denial of service by streaming data. Apache Tomcat Denial Of Service Vulnerability (Windows)						
Findings	Installed version 6.0.24Fixed version 6.0.377.0.30Installationpath port 8080tcp						
References	http://xforce.iss.net/xforce/xfdb/84144 http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-7.html http://svn.apache.org/viewvc?view=revision&revision=1476592 http://svn.apache.org/viewvc?view=revision&revision=1378921 http://svn.apache.org/viewvc?view=revision&revision=1378702						

CVE-2012-0022							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Apache Tomcat Server is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation could allow remote attackers to cause a denial of service via a specially crafted request.						
Solution	Upgrade Apache Tomcat to 5.5.35, 6.0.34, 7.0.23 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Apache Tomcat 5.5.x before 5.5.35, 6.x before 6.0.34, and 7.x before 7.0.23 uses an inefficient approach for handling parameters, which allows remote attackers to cause a denial of service (CPU consumption) via a request that contains many parameters and parameter values, a different vulnerability than CVE-2011-4858. Apache Tomcat Parameter Handling Denial of Service Vulnerability (Windows)						
Detection Method							
Findings	Installed version 6.0.24Fixed version 5.5.356.0.347.0.23Installationpath port 8080tcp						
References	http://tomcat.apache.org/security-5.html http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-7.html http://www.securityfocus.com/bid/51447						

<table>
<tr><th colspan="8">CVE-2018-15473</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>General</td><td></td><td><b>CVSS</b></td><td><b>5.0</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">OpenSSH is prone to a user enumeration vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.14 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6">Successfully exploitation will allow remote attacker to test   whether a certain user exists or not (username enumeration) on a target OpenSSH server.</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">Update to version 7.8 or later.</td><td colspan="2"><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
OpenSSH < 7.8 User Enumeration Vulnerability - Linux</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 6.6.1Fixed version   7.8Installationpath port   22tcp</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://0day.city/cve-2018-15473.html
https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2002-20001</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>Denial of Service</td><td></td><td><b>CVSS</b></td><td><b>5.0</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">The remote SSLTLS server is supporting Diffie-Hellman ephemeral DHE Key Exchange algorithms and thus could be prone to a denial of service DoS vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.46 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6"></td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">- DHE key exchange should be disabled if no other mitigation   mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should   be considered.   - Limit the maximum number of concurrent connections in e.g. the configuration of the remote   server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit'   option, for other products please refer to the manual of the product in question on configuration   possibilities.</td><td colspan="2"><b>Solution Type</b></td><td>Mitigation</td></tr>
<tr><th colspan="8">Additional Details</th></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE. Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks the supported cipher suites of the remote SSL/TLS   server.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">DHE cipher suites accepted by this service via the TLSv1.0 protocolTLSDHERSAWITH3DESEDECBCSHATLSDHERSAWITHAES256CBCSHATLSDHERSAWITHCAMELLIA256CBCSHADHE cipher suites accepted by this service via the TLSv1.1 protocolTLSDHERSAWITH3DESEDECBCSHATLSDHERSAWITHAES256CBCSHATLSDHERSAWITHCAMELLIA256CBCSHADHE cipher suites accepted by this service via the TLSv1.2 protocolTLSDHERSAWITH3DESEDECBCSHATLSDHERSAWITHAES256CBCSHATLSDHERSAWITHCAMELLIA256CBCSHA</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol
https://github.com/Balasys/dheater</td></tr>
</table>

Risk	Medium		Threat Type	Windows		CVSS	5.0
Summary	Distributed Computing Environment Remote Procedure Calls DCERPC or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.						
Affected Nodes	192.168.11.50 -						
Impact	An attacker may use this fact to gain more knowledge about the remote host.						
Solution	Filter incoming traffic to this ports.					Solution Type	Mitigation
Additional Details							
CVE Description	DCE/RPC and MSRPC Services Enumeration Reporting						

CVE-2013-2566							
Risk	Medium		Threat Type	SSL and TLS		CVSS	5.0
Summary	This routine reports all Weak SSLTLS cipher suites accepted by a service. NOTE No severity for SMTP services with Opportunistic TLS and weak cipher suites on port 25tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.						
Affected Nodes	192.168.11.50 -						
Impact							
Solution	The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.					Solution Type	Mitigation
Additional Details							
CVE Description	The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue. SSL/TLS: Report Weak Cipher Suites						
Detection Method							
Findings	Weak cipher suites accepted by this service via the TLSv1.0 protocolTLSRSAWITHRC4128MD5TLSRSAWITHRC4128SHAWeak cipher suites accepted by this service via the TLSv1.1 protocolTLSRSAWITHRC4128MD5TLSRSAWITHRC4128SHAWeak cipher suites accepted by this service via the TLSv1.2 protocolTLSRSAWITHRC4128MD5TLSRSAWITHRC4128SHA						
References	https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html https://bettercrypto.org/ https://mozilla.github.io/server-side-tls/ssl-config-generator/						

CVE-2011-0534							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary	Apache Tomcat is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to trigger a denial-of-service condition in the affected software.						
Solution	Upgrade Apache Tomcat version to 6.0.32, 7.0.8 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Apache Tomcat 7.0.0 through 7.0.6 and 6.0.0 through 6.0.30 does not enforce the maxHttpHeaderSize limit for requests involving the NIO HTTP connector, which allows remote attackers to cause a denial of service (OutOfMemoryError) via a crafted request. Apache Tomcat NIO Connector Denial of Service Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.327.0.8Installationpath port 8080tcp						
References	http://xforce.iss.net/xforce/xfdb/65162 http://www.securitytracker.com/id?1025027 http://cxsecurity.com/issue/WLB-2011020145						

CVE-2020-11881							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary	MikroTik RouterOS is prone to a denial of service vulnerability in the SMB server.						
Affected Nodes	192.168.11.62 -						
Impact							
Solution	Update to version 6.46.7 (long-term version)				**Solution Type**	VendorFix	
Additional Details							
CVE Description	An array index error in MikroTik RouterOS 6.41.3 through 6.46.5, and 7.x through 7.0 Beta5, allows an unauthenticated remote attacker to crash the SMB server via modified setup-request packets, aka SUP-12964. MikroTik RouterOS < 6.46.7, <= 6.47.3, 7.x DoS Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.47.10Fixed version None						
References	https://github.com/botlabsDev/CVE-2020-11881 https://forum.mikrotik.com/viewtopic.php?f=2&t=166137						

CVE-2001-1191							
Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	The remote web server dies when an URL ending with 2E is requested.						
Affected Nodes	192.168.11.21 -						
Impact	An attacker may use this flaw to make your server crash continually.						
Solution	Upgrade your server or firewall it.					Solution Type	VendorFix
Additional Details							
CVE Description	WebSeal in IBM Tivoli SecureWay Policy Director 3.8 allows remote attackers to cause a denial of service (crash) via a URL that ends in %2e. Webseal denial of service						

CVE-2002-1828							
Risk	Medium		Threat Type	Denial of Service		CVSS	5.0
Summary	The Savant web server was crashed by sending an invalid GET HTTP request with a negative Content-Length field.						
Affected Nodes	192.168.11.74 -						
Impact	An attacker may exploit this flaw to disable the service or even execute arbitrary code on the affected system.						
Solution	Upgrade the web server.					Solution Type	VendorFix
Additional Details							
CVE Description	Savant Webserver 3.1 allows remote attackers to cause a denial of service (crash) via an HTTP GET request with a negative Content-Length value. HTTP negative Content-Length DoS						

Risk	**Medium**		**Threat Type**	General		**CVSS**	**5.0**
Summary	The DNS server is prone to a cache snooping vulnerability.						
Affected Nodes	192.168.11.102 -						
Impact	Attackers might gain information about cached DNS records which might lead to further attacks. Note: This finding might be an acceptable risk if you: - trust all clients which can reach the server - do not allow recursive queries from outside your trusted client network.						
Solution	There are multiple possible mitigation steps depending on location and funcionality needed by the DNS server: - Disable recursion - Don't allow public access to DNS Servers doing recursion - Leave recursion enabled if the DNS Server stays on a corporate network that cannot be reached by untrusted clients				**Solution Type**	Mitigation	
Additional Details							
CVE Description	DNS Cache Snooping Vulnerability (UDP) - Active Check						
Detection Method	Sends a crafted DNS query and checks the response.						
Findings	Received an answers for a non-recursive query for example.com.						
References	https://www.cs.unc.edu/~fabian/course_papers/cache_snooping.pdf https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-server-cache-snooping-attacks https://kb.isc.org/docs/aa-00509 https://kb.isc.org/docs/aa-00482						

CVE-2000-0482							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**5.0**
Summary	The machine or a gateway on the network path crashed when flooded with incorrectly fragmented packets. This is known as the jolt2 denial of service attack.						
Affected Nodes	192.168.11.41 -						
Impact	An attacker may use this flaw to shut down this server or router, thus preventing you from working properly.						
Solution	Contact your operating system vendor for a patch.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Check Point Firewall-1 allows remote attackers to cause a denial of service by sending a large number of malformed fragmented IP packets. jolt2						

<table>
<tr><th colspan="8">CVE-2016-1907</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>Denial of Service</td><td></td><td><b>CVSS</b></td><td><b>5.0</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">openssh is prone to a denial of service DoS vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.14 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6">Successfully exploiting this issue allow   remote attackers to cause a denial of service (out-of-bounds read and application   crash).</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">Upgrade to OpenSSH version 7.1p2 or later.</td><td colspan="2"><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">The ssh_packet_read_poll2 function in packet.c in OpenSSH before 7.1p2 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted network traffic. OpenSSH Denial of Service Vulnerability - Jan16</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 6.6.1Fixed version   7.1p2Installationpath port   22tcp</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">http://www.openssh.com/txt/release-7.1p2
https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a789277bb0733ca36e1c0</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2002-20001</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>Denial of Service</td><td></td><td><b>CVSS</b></td><td><b>5.0</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">The remote SSH server is supporting Diffie-Hellman ephemeral DHE Key Exchange KEX algorithms and thus could be prone to a denial of service DoS vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.14 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6"></td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">- DHE key exchange should be disabled if no other mitigation   mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should   be considered.   - Limit the maximum number of concurrent connections in e.g. the configuration of the remote   server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products   please refer to the manual of the product in question on configuration possibilities.</td><td colspan="2"><b>Solution Type</b></td><td>Mitigation</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE. Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks the supported KEX algorithms of the remote SSH   server.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">The remote SSH server supports the following DHE KEX algorithmsdiffie-hellman-group1-sha1diffie-hellman-group14-sha1diffie-hellman-group-exchange-sha1diffie-hellman-group-exchange-sha256</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol
https://github.com/Balasys/dheater</td></tr>
</table>

Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Microsoft IIS Webserver is prone to an information disclosure vulnerability.						
Affected Nodes	192.168.11.110 -						
Impact	Successful exploitation will allow remote attackers to obtain sensitive information that could aid in further attacks.						
Solution	Disable the default pages within the server configuration.				**Solution Type**	Mitigation	
Additional Details							
CVE Description	Microsoft IIS Default Welcome Page Information Disclosure Vulnerability						
Detection Method							
Findings							
References							

CVE-2015-3200							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Lighttpd is prone to a remote code execution RCE vulnerability.						
Affected Nodes	192.168.11.76 -						
Impact	Successful exploitation will allow a remote attacker to execute arbitrary code on affected system.						
Solution	Upgrade to Lighttpd 1.4.36 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Mod_auth in lighttpd before 1.4.36 allows remote attackers to inject arbitrary log entries via a basic HTTP authentication string without a colon character, as demonstrated by a string containing a NULL and new line character. Lighttpd 'http_auth.c' Remote Code Execution Vulnerability - June15 (Linux)						
Detection Method	Check if the vulnerable version of Lighttpd is installed or not.						
Findings	Installed version 1.4.35Fixed version 1.4.36						
References	http://www.securitytracker.com/id/1032405 http://www.securityfocus.com/bid/74813 http://jaanuskp.blogspot.in/2015/05/cve-2015-3200.html						

Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Lighttpd is prone to an information disclosure and authentication bypass vulnerability.						
Affected Nodes	192.168.11.76 -						
Impact							
Solution	Upgrade to version 1.4.51 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Lighttpd < 1.4.51 Multiple Vulnerabilities						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.4.35Fixed version 1.4.51						
References	https://www.lighttpd.net/2018/10/14/1.4.51/						

CVE-2018-19052							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**5.0**
Summary	Lighttpd is prone to multiple path traversal and use-after-free vulnerabilities.						
Affected Nodes	192.168.11.76 -						
Impact	Successful exploitation might allow a remote attacker to execute arbitrary code on affected system or conduct path traversal attacks to get unauthorized access to files on the hosts filesystem.						
Solution	Upgrade to version 1.4.50 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	An issue was discovered in mod_alias_physical_handler in mod_alias.c in lighttpd before 1.4.50. There is potential ../ path traversal of a single directory above an alias target, with a specific mod_alias configuration where the matched alias lacks a trailing '/' character, but the alias target filesystem path does have a trailing '/' character. Lighttpd < 1.4.50 Multiple Vulnerabilities						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.4.35Fixed version 1.4.50						
References	https://www.lighttpd.net/2018/8/13/1.4.50/ https://redmine.lighttpd.net/issues/2898 https://github.com/lighttpd/lighttpd1.4/commit/2105dae0f9d7a964375ce681e53cb165375f84c1						

CVE-2018-15919							
Risk	Medium		Threat Type	General		CVSS	5.0
Summary		OpenSSH is prone to a user enumeration vulnerability.					
Affected Nodes		192.168.11.14 -					
Impact		Successfully exploitation will allow a remote attacker to harvest valid user accounts, which may aid in brute-force attacks.					
Solution		No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.			Solution Type		WillNotFix
Additional Details							
CVE Description		Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.' OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Linux					
Detection Method		Checks if a vulnerable version is present on the target host.					
Findings		Installed version 6.6.1Fixed version NoneInstallationpath port 22tcp					
References		https://bugzilla.novell.com/show_bug.cgi?id=1106163 https://seclists.org/oss-sec/2018/q3/180					

CVE-2017-15906							
Risk	**Medium**		**Threat Type**	General		**CVSS**	**5.0**
Summary	openssh is prone to a security bypass vulnerability.						
Affected Nodes	192.168.11.14 -						
Impact	Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.						
Solution	Upgrade to OpenSSH version 7.6 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files. OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version 7.6Installationpath port 22tcp						
References	https://www.openssh.com/txt/release-7.6 http://www.securityfocus.com/bid/101552 https://github.com/openbsd/src/commit/a6981567e8e						

CVE-2016-2183							
Risk	**Medium**		**Threat Type**	SSL and TLS		**CVSS**	**5.0**
Summary	This routine reports all SSLTLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.						
Affected Nodes	192.168.11.19 -						
Impact							
Solution	The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.				**Solution Type**		Mitigation
Additional Details							
CVE Description	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack. SSL/TLS: Report Vulnerable Cipher Suites for HTTPS						
Detection Method							
Findings	Vulnerable cipher suites accepted by this service via the TLSv1.0 protocolTLSRSAWITH3DESEDECBCSHA SWEET32Vulnerable cipher suites accepted by this service via the TLSv1.1 protocolTLSRSAWITH3DESEDECBCSHA SWEET32Vulnerable cipher suites accepted by this service via the TLSv1.2 protocolTLSRSAWITH3DESEDECBCSHA SWEET32						
References	https://bettercrypto.org/ https://mozilla.github.io/server-side-tls/ssl-config-generator/ https://sweet32.info/						

CVE-1999-0635							
Risk	Medium		Threat Type	Useless services		CVSS	5.0
Summary	An echo Service is running at this Host via TCP andor UDP.						
Affected Nodes	192.168.11.74 -						
Impact							
Solution	Disable the echo Service.				Solution Type		Mitigation
Additional Details							
CVE Description	The echo service is running. echo Service Reporting (TCP + UDP)						
Detection Method							
Findings							
References							

Risk	Medium		Threat Type	General		CVSS	4.8
Summary	The remote host is running a FTP service that allows cleartext logins over unencrypted connections.						
Affected Nodes	192.168.11.62 -						
Impact	An attacker can uncover login names and passwords by sniffing traffic to the FTP service.						
Solution	Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.				Solution Type		Mitigation
Additional Details							
CVE Description	FTP Unencrypted Cleartext Login						
Detection Method	Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.						
Findings	The remote FTP service accepts logins without a previous sent AUTH TLS command. ResponsesNon-anonymous sessions 331 Password required for openvasvtAnonymous sessions 331 Password required for anonymous						
References							

Risk	**Medium**		**Threat Type**	General		**CVSS**	**4.8**
Summary	The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Types not intended for use on untrusted networks.						
Affected Nodes	192.168.11.48 -						
Impact	An attacker can uncover sensitive data by sniffing traffic to the VNC server.						
Solution	Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.					**Solution Type**	Mitigation
Additional Details							
CVE Description	VNC Server Unencrypted Data Transmission						
Detection Method							
Findings	The VNC server provides the following insecure or cryptographically weak Security Types2 VNC authentication						
References	https://tools.ietf.org/html/rfc6143#page-10						

Risk	**Medium**		**Threat Type**	General		**CVSS**	**4.8**
Summary	The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.						
Affected Nodes	192.168.11.74 -						
Impact	An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.						
Solution	Replace Telnet with a protocol like SSH which supports encrypted connections.					**Solution Type**	Mitigation
Additional Details							
CVE Description	Telnet Unencrypted Cleartext Login						
Detection Method							
Findings							
References							

Risk	**Medium**		**Threat Type**	Web application abuses		**CVSS**	**4.8**
Summary	The host application transmits sensitive information username passwords in cleartext via HTTP.						
Affected Nodes	192.168.11.86 -						
Impact	An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.						
Solution	Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.				**Solution Type**	Workaround	
Additional Details							
CVE Description	Cleartext Transmission of Sensitive Information via HTTP						
Detection Method	Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type 'password'						
Findings	The following URLs requires Basic Authentication URLrealm namehttp192.168.11.868080host-managerhtmlTomcat Host Manager Applicationhttp192.168.11.868080managerhtmlTomcat Manager Applicationhttp192.168.11.868080managerstatusTomcat Manager Application						
References	https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure https://cwe.mitre.org/data/definitions/319.html						

<table>
<tr><th colspan="8">CVE-2017-9079</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>General</td><td></td><td>CVSS</td><td>4.7</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Dropbear SSH is prone to a local file read vulnerability via symlinks.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.22 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">Successfully exploiting this issue might allow local users to read certain files as root, if the file has the authorized_keys file format with a command= option.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="4">Update to Dropbear SSH version 2017.75 or later.</td><td>Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Dropbear before 2017.75 might allow local users to read certain files as root, if the file has the authorized_keys file format with a command= option. This occurs because ~/.ssh/authorized_keys is read with root privileges and symlinks are followed.
Dropbear SSH Symlink Local File Read Vulnerability (CVE-2017-9079)</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 2015.68Fixed version 2017.75Installationpath port 2400tcp</td></tr>
<tr><td colspan="2">References</td><td colspan="6">https://lists.ucc.gu.uwa.edu.au/pipermail/dropbear/2017q2/001985.html
https://matt.ucc.asn.au/dropbear/CHANGES</td></tr>
</table>

<table>
<tr><th colspan="8"></th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>General</td><td></td><td>CVSS</td><td>4.6</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">The remote SSH server uses a weak too small public key size.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.1.2 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">A man-in-the-middle attacker can exploit this vulnerability to record the communication to decrypt the session key and even the messages.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="4">- <= 1024 bit for RSA based keys:
Install a RSA public key length of 2048 bits or greater, or to switch to more secure key types.</td><td>Solution Type</td><td>Mitigation</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Weak (Small) Public Key Size(s) (SSH)</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks the public key size of the remote SSH server. Currently weak (too small) key sizes are defined as the following: - <= 1024 bit for RSA based keys</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">The remote SSH server uses a public RSA key with the following weak too small size 1024</td></tr>
<tr><td colspan="2">References</td><td colspan="6">https://www.linuxminion.com/ssh-server-public-key-too-small/</td></tr>
</table>

Risk	Medium		Threat Type	General		CVSS	4.6
Summary	The remote SSH server is configured to allow support weak host key algorithms.						
Affected Nodes	192.168.11.14 -						
Impact							
Solution	Disable the reported weak host key algorithm(s).					Solution Type	Mitigation
Additional Details							
CVE Description	Weak Host Key Algorithm(s) (SSH)						
Detection Method	Checks the supported host key algorithms of the remote SSH server. Currently weak host key algorithms are defined as the following: - ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)						
Findings	The remote SSH server supports the following weak host key algorithmshost key algorithm Description--ssh-dss Digital Signature Algorithm DSA Digital Signature Standard DSS						
References							

<table>
<tr><th colspan="8">CVE-2016-0777</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>General</td><td></td><td><b>CVSS</b></td><td><b>4.6</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">The OpenSSH client code between 5.4 and 7.1p1 contains experimental support for resuming SSH-connections roaming. The matching server code has never been shipped but the client code was enabled by default and could be tricked by a malicious server into leaking client memory to the server including private client user keys. The authentication of the server host key prevents exploitation by a man-in-the-middle so this information leak is restricted to connections to malicious or compromised servers.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.14 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6"></td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">Update to 7.1p2 or newer.</td><td colspan="2"><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings. OpenSSH Client Information Leak</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 6.6.1Fixed version   7.1p2Installationpath port   22tcp</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">http://www.openssh.com/txt/release-7.1p2</td></tr>
</table>

Risk	**Medium**		**Threat Type**	General		**CVSS**	**4.6**
Summary	The remote SSH server is configured to allow support weak key exchange KEX algorithms.						
Affected Nodes	192.168.11.22 -						
Impact	An attacker can quickly break individual connections.						
Solution	Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.					**Solution Type**	Mitigation
Additional Details							
CVE Description	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)						
Detection Method	Checks the supported KEX algorithms of the remote SSH server. Currently weak KEX algorithms are defined as the following: - non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime - ephemerally generated key exchange groups uses SHA-1 - using RSA 1024-bit modulus key						
Findings	The remote SSH server supports the following weak KEX algorithmsKEX algorithm Reason--diffie-hellman-group1-sha1 Using Oakley Group 2 a 1024-bit MODP group and SHA-1						
References	https://weakdh.org/sysadmin.html https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.section.5 https://datatracker.ietf.org/doc/html/rfc6194						

CVE-2011-2526							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**4.4**
Summary	Apache Tomcat is prone to a remote information-disclosure vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Remote attackers can exploit this issue to obtain sensitive information that will aid in further attacks. Attackers may also crash the JVM.						
Solution	Updates are available. Please see the references for more information.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.19, when sendfile is enabled for the HTTP APR or HTTP NIO connector, does not validate certain request attributes, which allows local users to bypass intended file access restrictions or cause a denial of service (infinite loop or JVM crash) by leveraging an untrusted web application. Apache Tomcat 'sendfile' Request Attributes Information Disclosure Vulnerability						
Detection Method							
Findings	Installed version 6.0.24Fixed version 5.5.346.0.337.0.19Installationpath port 8080tcp						
References	http://www.securityfocus.com/bid/48667 http://tomcat.apache.org/security-5.html http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-7.html http://www.ibm.com/support/docview.wss?uid=swg21507512 http://support.avaya.com/css/P8/documents/100147767						

<table>
<tr><th colspan="8">CVE-2019-16905</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>General</td><td></td><td>CVSS</td><td>4.4</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">OpenSSH is prone to an integer overflow vulnerability.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.141 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">Successfully exploitation could lead to memory corruption and local code execution.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Update to version 8.1 or later.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH. OpenSSH < 8.1 Integer Overflow Vulnerability</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 7.9Fixed version 8.1Installationpath port 22tcp</td></tr>
<tr><td colspan="2">References</td><td colspan="6">https://www.openssh.com/txt/release-8.1
https://0day.life/exploits/0day-1009.html
https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/sshkey-xmss.c.diff?r1=1.5&r2=1.6&f=h</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2019-12522</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>General</td><td></td><td><b>CVSS</b></td><td><b>4.4</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">Squid is prone to a privilege escalation vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.1.251 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6">This behaviour makes it trivial for an attacker who has   compromised the child process to escalate their privileges back to root.</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.</td><td colspan="2"><b>Solution Type</b></td><td>WillNotFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">An issue was discovered in Squid through 4.7. When Squid is run as root, it spawns its child processes as a lesser user, by default the user nobody. This is done via the leave_suid call. leave_suid leaves the Saved UID as 0. This makes it trivial for an attacker who has compromised the child process to escalate their privileges back to root. Squid Proxy Cache <= 4.14 Privilege Escalation Vulnerability</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 3.5.20Fixed version   No known solutionInstallationpath port 3128tcp</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://gitlab.com/jeriko.one/security/-/blob/master/squid/CVEs/CVE-2019-12522.txt</td></tr>
</table>

CVE-2021-41617							
Risk	Medium		Threat Type	Privilege escalation		CVSS	4.4
Summary	OpenSSH is prone to a privilege scalation vulnerability in certain configurations.						
Affected Nodes	192.168.11.19 -						
Impact							
Solution	Update to version 8.8 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	Sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user. OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 7.1Fixed version 8.8Installationpath port 22tcp						
References	https://www.openssh.com/txt/release-8.8						

CVE-2015-5352							
Risk	Medium		Threat Type	General		CVSS	4.3
Summary	OpenSSH is prone to a security bypass vulnerability.						
Affected Nodes	192.168.11.14 -						
Impact	Successful exploitation will allow remote attackers to bypass intended access restrictions.						
Solution	Upgrade to OpenSSH version 6.9 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window. OpenSSH Security Bypass Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version 6.9Installationpath port 22tcp						
References	http://openwall.com/lists/oss-security/2015/07/01/10						

CVE-2020-11022							
Risk	Medium		Threat Type	Web application abuses		CVSS	4.3
Summary	jQuery is prone to a cross-site scripting XSS vulnerability in jQuery.htmlPrefilter and related methods.						
Affected Nodes	192.168.6.252 -						
Impact							
Solution	Update to version 3.5.0 or later.				Solution Type	VendorFix	
Additional Details							
CVE Description	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. jQuery 1.2 < 3.5.0 XSS Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.12.4Fixed version 3.5.0Installationpath port wwwjs						
References	https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2						

CVE-2019-5428							
Risk	Medium		Threat Type	Web application abuses		CVSS	4.3
Summary	jQuery is prone to multiple vulnerabilities regarding property injection in Object.prototype.						
Affected Nodes	192.168.6.252 -						
Impact							
Solution	Update to version 3.4.0 or later. Patch diffs are available for older versions.				Solution Type	VendorFix	
Additional Details							
CVE Description	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-11358. Reason: This candidate is a duplicate of CVE-2019-11358. Notes: All CVE users should reference CVE-2019-11358 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage. jQuery < 3.4.0 Object Extensions Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.12.4Fixed version 3.4.0Installationpath port wwwjs						
References	https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://github.com/DanielRuf/snyk-js-jquery-174006?files=1						

<table>
<tr><th colspan="8">CVE-2016-20012</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>General</td><td></td><td><b>CVSS</b></td><td><b>4.3</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">OpenBSD OpenSSH is prone to an information disclosure vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.14 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6"></td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.</td><td colspan="2"><b>Solution Type</b></td><td>NoneAvailable</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">** DISPUTED ** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product. OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 6.6.1Fixed version NoneInstallationpath port 22tcp</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://github.com/openssh/openssh-portable/pull/270
https://rushter.com/blog/public-ssh-keys/
https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak</td></tr>
</table>

CVE-2019-14834							
Risk	Medium		Threat Type	Denial of Service		CVSS	4.3
Summary	Dnsmasq is prone to a Denial of Service DoS vulnerability.						
Affected Nodes	192.168.9.170 -						
Impact	The memory leak allows remote attackers to cause a DoS (memory consumption) via vectors involving DHCP response creation.						
Solution	Update to version 2.81 or later.	Solution Type	VendorFix				
Additional Details							
CVE Description	A vulnerability was found in dnsmasq before version 2.81, where the memory leak allows remote attackers to cause a denial of service (memory consumption) via vectors involving DHCP response creation. Dnsmasq < 2.81 DoS Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 2.80Fixed version 2.81Installationpath port 53udp						
References	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14834 http://thekelleys.org.uk/dnsmasq/CHANGELOG						

Risk	Medium		Threat Type	General		CVSS	4.3
Summary	The remote SSH server is configured to allow support weak encryption algorithms.						
Affected Nodes	192.168.11.14 -						
Impact							
Solution	Disable the reported weak encryption algorithm(s).	Solution Type	Mitigation				
Additional Details							
CVE Description	Weak Encryption Algorithm(s) Supported (SSH)						
Detection Method	Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak encryption algorithms are defined as the following: - Arcfour (RC4) cipher based algorithms - none algorithm - CBC mode cipher based algorithms						
Findings	The remote SSH server supports the following weak client-to-server encryption algorithms3des-cbcThe remote SSH server supports the following weak server-to-client encryption algorithms3des-cbc						
References	https://tools.ietf.org/html/rfc4253#section-6.3 https://www.kb.cert.org/vuls/id/958563						

<table>
<tr><th colspan="8">CVE-2021-3448</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>General</td><td></td><td>CVSS</td><td>4.3</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Dnsmasq is prone to a DNS cache poisoning vulnerability.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.9.170 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6"></td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Update to version 2.85 or later.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">A flaw was found in dnsmasq in versions before 2.85. When configured to use a specific server for a given network interface, dnsmasq uses a fixed port while forwarding queries. An attacker on the network, able to find the outgoing port used by dnsmasq, only needs to guess the random transmission ID to forge a reply and get it accepted by dnsmasq. This flaw makes a DNS Cache Poisoning attack much easier. The highest threat from this vulnerability is to data integrity. Dnsmasq < 2.85 DNS Cache Poisoning Vulnerability</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 2.80Fixed version 2.85Installationpath port 53udp</td></tr>
<tr><td colspan="2">References</td><td colspan="6">https://lists.thekelleys.org.uk/pipermail/dnsmasq-discuss/2021q2/014962.html
https://bugzilla.redhat.com/show_bug.cgi?id=1939368
https://www.thekelleys.org.uk/dnsmasq/CHANGELOG</td></tr>
</table>

CVE-2020-14145							
Risk	**Medium**		**Threat Type**	General		**CVSS**	**4.3**
Summary	OpenBSD OpenSSH is prone to an information disclosure vulnerability.						
Affected Nodes	192.168.11.14 -						
Impact							
Solution	Update to version 8.5 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected. OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.6.1Fixed version 8.5Installationpath port 22tcp						
References	http://www.openwall.com/lists/oss-security/2020/12/02/1						

CVE-2022-22707							
Risk	Medium		Threat Type	Web Servers		CVSS	4.3
Summary	Lighttpd is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.6.252 -						
Impact							
Solution	No known solution is available as of 11th January, 2022. Information regarding this issue will be updated once solution details are available.				Solution Type		NoneAvailable
Additional Details							
CVE Description	In lighttpd 1.4.46 through 1.4.63, the mod_extforward_Forwarded function of the mod_extforward plugin has a stack-based buffer overflow (4 bytes representing -1), as demonstrated by remote denial of service (daemon crash) in a non-default configuration. The non-default configuration requires handling of the Forwarded header in a somewhat unusual manner. Also, a 32-bit system is much more likely to be affected than a 64-bit system. Lighttpd 1.4.46 - 1.4.63 DoS Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.4.49Fixed version None						
References	https://redmine.lighttpd.net/issues/3134						

CVE-2015-9251							
Risk	Medium		Threat Type	Web application abuses		CVSS	4.3
Summary	jQuery is vulnerable to Cross-site Scripting XSS attacks.						
Affected Nodes	192.168.6.252 -						
Impact							
Solution	Update to version 3.0.0 or later or apply the patch.				Solution Type		VendorFix
Additional Details							
CVE Description	JQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed. jQuery < 3.0.0 XSS Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.12.4Fixed version 3.0.0Installationpath port wwwjs						
References	https://github.com/jquery/jquery/issues/2432						

<table>
<tr><th colspan="8">CVE-2013-3587</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>SSL and TLS</td><td></td><td>CVSS</td><td>4.3</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">SSLTLS connections are vulnerable to the BREACH Browser Reconnaissance Exfiltration via Adaptive Compression of Hypertext attack.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.21 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6">The flaw makes it easier for man-in-the-middle attackers to obtain plaintext secret values.</td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">The following mitigation possibilities are available: 1. Disabling HTTP compression 2. Separating secrets from user input 3. Randomizing secrets per request 4. Masking secrets (effectively randomizing by XORing with a random secret per request) 5. Protecting vulnerable pages with CSRF 6. Length hiding (by adding random number of bytes to the responses) 7. Rate-limiting the requests Note: The mitigations are ordered by effectiveness (not by their practicality - as this may differ from one application to another).</td><td colspan="2">Solution Type</td><td>Mitigation</td></tr>
<tr><th colspan="8">Additional Details</th></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">The HTTPS protocol, as used in unspecified web applications, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which makes it easier for man-in-the-middle attackers to obtain plaintext secret values by observing length differences during a series of guesses in which a string in an HTTP request URL potentially matches an unknown string in an HTTP response body, aka a "BREACH" attack, a different issue than CVE-2012-4929. SSL/TLS: BREACH attack against HTTP compression</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if the remote web server has HTTP compression enabled. Note: Even with HTTP compression enabled the web application hosted on the web server might not be vulnerable. The low Quality of Detection (QoD) of this VT reflects this fact.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Based on the following information it was determined that the remote web server has HTTP compression enabledHTTP headers Content-encoding gzipURL https192.168.11.21</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://breachattack.com/
http://www.kb.cert.org/vuls/id/987798
http://www.openwall.com/lists/oss-security/2013/08/07/1
https://bugzilla.redhat.com/show_bug.cgi?id=995168
https://en.wikipedia.org/wiki/HTTP_compression</td></tr>
</table>

CVE-2020-11023							
Risk	Medium		Threat Type	Web application abuses		CVSS	4.3
Summary	jQuery is prone to a cross-site scripting XSS vulnerability when appending HTML containing option elements.						
Affected Nodes	192.168.6.252 -						
Impact							
Solution	Update to version 3.5.0 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing &amp;lt;option&amp;gt; elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. jQuery 1.0.3 < 3.5.0 XSS Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.12.4Fixed version 3.5.0Installationpath port wwwjs						
References	https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6						

CVE-2016-5331							
Risk	Medium		Threat Type	General		CVSS	4.3
Summary	ESXi contain an HTTP header injection vulnerability due to lack of input validation. An attacker can exploit this issue to set arbitrary HTTP response headers and cookies which may allow for cross-site scripting and malicious redirect attacks.						
Affected Nodes	192.168.11.14 -						
Impact							
Solution	Apply the missing patch(es).					Solution Type	VendorFix
Additional Details							
CVE Description	CRLF injection vulnerability in VMware vCenter Server 6.0 before U2 and ESXi 6.0 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors. VMSA-2016-0010 (CVE-2016-5331) ESXi: VMware product updates address multiple important security issues (remote check)						
Detection Method	Check the build number.						
Findings	ESXi Version 6.0.0Detected Build 2494585Fixed Build 3568943						
References	http://www.vmware.com/security/advisories/VMSA-2016-0010.html						

<table>
<tr><th colspan="8">CVE-2021-28116</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>Web application abuses</td><td></td><td><b>CVSS</b></td><td><b>4.3</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">Squid is prone to an information disclosure vulnerability.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.1.251 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6">Successful exploitation would allow an attacker to read sensitive information.</td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">Update to version 4.17, 5.2 or later.</td><td colspan="2"><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">Squid through 4.14 and 5.x through 5.0.5, in some configurations, allows information disclosure because of an out-of-bounds read in WCCP protocol data. This can be leveraged as part of a chain for remote code execution as nobody. Squid Information Disclosure Vulnerability (SQUID-2020:12)</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 3.5.20Fixed version 4.17Installationpath port 3128tcp</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://www.openwall.com/lists/oss-security/2021/10/04/1
https://www.zerodayinitiative.com/advisories/ZDI-21-157/</td></tr>
</table>

CVE-2016-0800							
Risk	Medium		Threat Type	SSL and TLS		CVSS	4.3
Summary	It was possible to detect the usage of the deprecated SSLv2 andor SSLv3 protocol on this system.						
Affected Nodes	192.168.11.14 -						
Impact	An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.						
Solution	It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.				Solution Type		Mitigation
Additional Details							
CVE Description	The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack. SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection						
Detection Method	Check the used SSL protocols of the services provided by this system.						
Findings	In addition to TLSv1.0 the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the SSLTLS Report Supported Cipher Suites OID 1.3.6.1.4.1.25623.1.0.802067 VT.						
References	https://ssl-config.mozilla.org/ https://bettercrypto.org/ https://drownattack.com/ https://www.imperialviolet.org/2014/10/14/poodle.html https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014						

<table>
<tr><th colspan="8">CVE-2019-12529</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>Denial of Service</td><td></td><td>CVSS</td><td>4.3</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Squid is prone to a denial of service vulnerability due to incorrect buffer management when processing HTTP Basic Authentication credentials.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.1.251 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6"></td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Update to version 4.8 or later.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">An issue was discovered in Squid 2.x through 2.7.STABLE9, 3.x through 3.5.28, and 4.x through 4.7. When Squid is configured to use Basic Authentication, the Proxy-Authorization header is parsed via uudecode. uudecode determines how many bytes will be decoded by iterating over the input and checking its table. The length is then used to start decoding the string. There are no checks to ensure that the length it calculates isn't greater than the input buffer. This leads to adjacent memory being decoded as well. An attacker would not be able to retrieve the decoded data unless the Squid maintainer had configured the display of usernames on error pages. Squid Proxy Cache Security Update Advisory SQUID-2019:2</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 3.5.20Fixed version   4.8</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://www.squid-cache.org/Advisories/SQUID-2019_2.txt</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2013-1571</th></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>Web Servers</td><td></td><td><b>CVSS</b></td><td><b>4.3</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">Apache Tomcat is prone to a frame injection vulnerability in Javadoc.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.86 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6"></td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="3">Update to version 6.0.39 or later.</td><td colspan="2"><b>Solution Type</b></td><td>VendorFix</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">Unspecified vulnerability in the Javadoc component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier; JavaFX 2.2.21 and earlier; and OpenJDK 7 allows remote attackers to affect integrity via unknown vectors related to Javadoc. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to frame injection in HTML that is generated by Javadoc. Apache Tomcat Java Vulnerability (Jan 2014) - Windows</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">Installed version 6.0.24Fixed version 6.0.39Installationpath port 8080tcp</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://tomcat.apache.org/security-6.html</td></tr>
</table>

CVE-2013-4322							
Risk	Medium		Threat Type	Web Servers		CVSS	4.3
Summary	Apache Tomcat is prone to multiple vulnerabilities.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to gain access to potentially sensitive internal information or crash the program.						
Solution	Upgrade to version 6.0.39 or 7.0.50 or 8.0.0-RC10 or later.					Solution Type	VendorFix
Additional Details							
CVE Description	Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 processes chunked transfer coding without properly handling (1) a large total amount of chunked data or (2) whitespace characters in an HTTP header value within a trailer field, which allows remote attackers to cause a denial of service by streaming data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-3544. Apache Tomcat Multiple Vulnerabilities - 02 - Mar14						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.397.0.508.0.0-RC10Installationpath port 8080tcp						
References	http://seclists.org/bugtraq/2014/Feb/132 http://seclists.org/bugtraq/2014/Feb/133 http://packetstormsecurity.com/files/125400 http://packetstormsecurity.com/files/125404						

CVE-2011-3389							
Risk	**Medium**		**Threat Type**	SSL and TLS		**CVSS**	**4.3**
Summary	It was possible to detect the usage of the deprecated TLSv1.0 andor TLSv1.1 protocol on this system.						
Affected Nodes	192.168.11.19 -						
Impact	An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.						
Solution	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.					**Solution Type**	Mitigation
Additional Details							
CVE Description	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack. SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection						
Detection Method	Check the used TLS protocols of the services provided by this system.						
Findings	In addition to TLSv1.2 the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the SSLTLS Report Supported Cipher Suites OID 1.3.6.1.4.1.25623.1.0.802067 VT.						
References	https://ssl-config.mozilla.org/ https://bettercrypto.org/ https://datatracker.ietf.org/doc/rfc8996/ https://vnhacker.blogspot.com/2011/09/beast.html https://web.archive.org/web/20201108095603/https://censys.io/blog/freak https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014						

CVE-2019-13345							
Risk	**Medium**		**Threat Type**	Web application abuses		**CVSS**	**4.3**
Summary	Squid is prone to multiple cross-site scripting vulnerabilities due to incorrect input handling in the cachemgr.cgi tool.						
Affected Nodes	192.168.1.251 -						
Impact							
Solution	Update to version 4.8 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	The cachemgr.cgi web module of Squid through 4.7 has XSS via the user_name or auth parameter. Squid Proxy Cache Security Update Advisory SQUID-2019:6						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.8						
References	http://www.squid-cache.org/Advisories/SQUID-2019_6.txt						

CVE-2018-19132							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**4.3**
Summary	Squid is prone to a denial of service vulnerability due to a memory leak in the SNMP query rejection code.						
Affected Nodes	192.168.1.251 -						
Impact							
Solution	Update to version 4.4 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Squid before 4.4, when SNMP is enabled, allows a denial of service (Memory Leak) via an SNMP packet. Squid Proxy Cache Security Update Advisory SQUID-2018:5						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.4						
References	http://www.squid-cache.org/Advisories/SQUID-2018_5.txt						

CVE-2010-4172							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**4.3**
Summary	Apache Tomcat is prone to multiple cross-site scripting vulnerabilities because it fails to properly sanitize user-supplied input.						
Affected Nodes	192.168.11.86 -						
Impact	An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker steal cookie-based authentication credentials and launch other attacks.						
Solution	Updates are available. Please see the references for more information.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Multiple cross-site scripting (XSS) vulnerabilities in the Manager application in Apache Tomcat 6.0.12 through 6.0.29 and 7.0.0 through 7.0.4 allow remote attackers to inject arbitrary web script or HTML via the (1) orderBy or (2) sort parameter to sessionsList.jsp, or unspecified input to (3) sessionDetail.jsp or (4) java/org/apache/catalina/manager/JspHelper.java, related to use of untrusted web applications. Apache Tomcat 'sort' and 'orderBy' Parameters Cross Site Scripting Vulnerabilities						
Detection Method							
Findings	Installed version 6.0.24Fixed version 6.0.307.0.5Installationpath port 8080tcp						
References	http://www.securityfocus.com/bid/45015 http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-7.html http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-7.html http://www.securityfocus.com/archive/1/514866						

CVE-2014-3566							
Risk	**Medium**		**Threat Type**	SSL and TLS		**CVSS**	**4.3**
Summary	This host is prone to an information disclosure vulnerability.						
Affected Nodes	192.168.1.20 -						
Impact	Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.						
Solution	Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+					**Solution Type**	Mitigation
Additional Details							
CVE Description	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)						
Detection Method	Evaluate previous collected information about this service.						
Findings							
References	https://www.openssl.org/~bodo/ssl-poodle.pdf https://www.imperialviolet.org/2014/10/14/poodle.html https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html						

<table>
<tr><th colspan="8">CVE-2019-18860</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>Web application abuses</td><td></td><td>CVSS</td><td>4.3</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Squid when certain web browsers are used mishandles HTML in the host aka hostname parameter to cachemgr.cgi.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.1.251 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6"></td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Update to version 4.9 or later.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Squid before 4.9, when certain web browsers are used, mishandles HTML in the host (aka hostname) parameter to cachemgr.cgi. Squid Proxy Cache < 4.9 Hostname Validation Vulnerability</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 3.5.20Fixed version 4.9</td></tr>
<tr><td colspan="2">References</td><td colspan="6">https://github.com/squid-cache/squid/pull/504
https://github.com/squid-cache/squid/pull/505</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2018-19131</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>Web application abuses</td><td></td><td>CVSS</td><td>4.3</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">Squid is prone to a cross-site scripting vulnerability to incorrect input handling when generating HTTPS response messages about TLS errors.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.1.251 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6"></td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">Update to version 4.4 or later.</td><td colspan="2">Solution Type</td><td>VendorFix</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Squid before 4.4 has XSS via a crafted X.509 certificate during HTTP(S) error page generation for certificate errors. Squid Proxy Cache Security Update Advisory SQUID-2018:4</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 3.5.20Fixed version 4.4</td></tr>
<tr><td colspan="2">References</td><td colspan="6">http://www.squid-cache.org/Advisories/SQUID-2018_4.txt</td></tr>
</table>

CVE-2018-1172							
Risk	**Medium**		**Threat Type**	Web application abuses		**CVSS**	**4.3**
Summary	Squid is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.1.251 -						
Impact	Successful exploitation will allow remote attackers to cause a denial of service.						
Solution	Upgrade to Squid version 4.0.13 or later. Patch and workaround is also available. Please see the references for more information.					**Solution Type**	VendorFix
Additional Details							
CVE Description	This vulnerability allows remote attackers to deny service on vulnerable installations of The Squid Software Foundation Squid 3.5.27-20180318. Authentication is not required to exploit this vulnerability. The specific flaw exists within ClientRequestContext::sslBumpAccessCheck(). A crafted request can trigger the dereference of a null pointer. An attacker can leverage this vulnerability to create a denial-of-service condition to users of the system. Was ZDI-CAN-6088. Squid Proxy Cache Denial of Service Vulnerability (SQUID-2018:3)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.0.13Installationpath port 3128tcp						
References	http://www.squid-cache.org/Advisories/SQUID-2018_3.txt						

CVE-2014-0119							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**4.3**
Summary	Apache Tomcat is prone to an information disclosure vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference.						
Solution	Update to version 6.0.40, 7.0.54, 8.0.6 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Apache Tomcat before 6.0.40, 7.x before 7.0.54, and 8.x before 8.0.6 does not properly constrain the class loader that accesses the XML parser used with an XSLT stylesheet, which allows remote attackers to (1) read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, or (2) read files associated with different web applications on a single Tomcat instance via a crafted web application. Apache Tomcat Information Disclosure Vulnerability (May 2014)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.407.0.538.0.5Installationpath port 8080tcp						
References	http://secunia.com/advisories/59732 http://tomcat.apache.org/security-8.html http://tomcat.apache.org/security-7.html http://tomcat.apache.org/security-6.html						

CVE-2016-5331							
Risk	Medium		Threat Type	Web application abuses		CVSS	4.3
Summary	ESXi contain an HTTP header injection vulnerability due to lack of input validation. An attacker can exploit this issue to set arbitrary HTTP response headers and cookies which may allow for cross-site scripting and malicious redirect attacks.						
Affected Nodes	192.168.11.14 -						
Impact							
Solution	Apply the missing patch(es).				Solution Type		VendorFix
Additional Details							
CVE Description	CRLF injection vulnerability in VMware vCenter Server 6.0 before U2 and ESXi 6.0 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors. VMSA-2016-0010 (CVE-2016-5331) ESXi: VMware product updates address multiple important security issues (remote active check)						
Detection Method	Send a special crafted HTTP GET request and check the response.						
Findings	Vulnerable URL https192.168.11.14syss0d0aSet-Cookie20OpenVASVT11411747790d0aopenvasvt201222744051ResponseHTTP1.1 303 See OtherDate Sun 10 Apr 2022 123849 GMTConnection closeLocation syssSet-Cookie OpenVASVT1141174779openvasvt 1222744051Content-Length 0						
References	http://www.vmware.com/security/advisories/VMSA-2016-0010.html						

CVE-2021-31806							
Risk	Medium		Threat Type	Denial of Service		CVSS	4.0
Summary	Squid is prone to multiple denial of service DoS vulnerabilities.						
Affected Nodes	192.168.1.251 -						
Impact							
Solution	Update to version 4.15, 5.0.6 or later.				Solution Type		VendorFix
Additional Details							
CVE Description	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. An integer overflow problem allows a remote server to achieve Denial of Service when delivering responses to HTTP Range requests. The issue trigger is a header that can be expected to exist in HTTP traffic without any malicious intent. Squid 2.5.STABLE2 < 4.15, 5.0.1 < 5.0.6 Multiple DoS Vulnerabilities (SQUID-2021:4)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.15Installationpath port 3128tcp						
References	https://github.com/squid-cache/squid/security/advisories/GHSA-pxwq-f3qr-w2xf						

CVE-2021-28652							
Risk	Medium		Threat Type	Denial of Service		CVSS	4.0
Summary	Squid is prone to a denial of service DoS vulnerability in the Cache Manager.						
Affected Nodes	192.168.1.251 -						
Impact							
Solution	Update to version 4.15, 5.0.6 or later. See the referenced vendor advisory for a workaround.				Solution Type	VendorFix	
Additional Details							
CVE Description	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. Due to incorrect parser validation, it allows a Denial of Service attack against the Cache Manager API. This allows a trusted client to trigger memory leaks that. over time, lead to a Denial of Service via an unspecified short query string. This attack is limited to clients with Cache Manager API access privilege. Squid 1.0 < 4.14, 5.0 < 5.0.5 DoS Vulnerability (SQUID-2021:3)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.15Installationpath port 3128tcp						
References	https://github.com/squid-cache/squid/security/advisories/GHSA-m47m-9hvw-7447						

CVE-2021-33620							
Risk	Medium		Threat Type	Denial of Service		CVSS	4.0
Summary	Squid is prone to a denial of service DoS vulnerability.						
Affected Nodes	192.168.1.251 -						
Impact							
Solution	Update to version 4.15, 5.0.6 or later.				Solution Type	VendorFix	
Additional Details							
CVE Description	Squid before 4.15 and 5.x before 5.0.6 allows remote servers to cause a denial of service (affecting availability to all clients) via an HTTP response. The issue trigger is a header that can be expected to exist in HTTP traffic without any malicious intent by the server. Squid < 4.15, 5.0.x < 5.0.6 DoS Vulnerability (SQUID-2021:5)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.15Installationpath port 3128tcp						
References	https://github.com/squid-cache/squid/security/advisories/GHSA-572g-rvwr-6c7f						

CVE-2020-15810							
Risk	**Medium**		**Threat Type**	Denial of Service		**CVSS**	**4.0**
Summary	Squid is prone to multiple vulnerabilities.						
Affected Nodes	192.168.1.251 -						
Impact	These vulnerabilities may lead to cache poisoning.						
Solution	Update to version 4.13, 5.0.4 or later.				**Solution Type**		VendorFix
Additional Details							
CVE Description	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Splitting attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the browser cache and any downstream caches with content from an arbitrary source. Squid uses a string search instead of parsing the Transfer-Encoding header to find chunked encoding. This allows an attacker to hide a second request inside Transfer-Encoding: it is interpreted by Squid as chunked and split out into a second request delivered upstream. Squid will then deliver two distinct responses to the client, corrupting any downstream caches. Squid Proxy Cache Security Update Advisory SQUID-2020:8 SQUID-2020:10						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 3.5.20Fixed version 4.13						
References	https://github.com/squid-cache/squid/security/advisories/GHSA-3365-q9qx-f98m https://github.com/squid-cache/squid/security/advisories/GHSA-c7p8-xqhm-49wv						

<table>
<tr><td colspan="8"></td></tr>
<tr><td><b>Risk</b></td><td><b>Medium</b></td><td></td><td><b>Threat Type</b></td><td>SSL and TLS</td><td></td><td><b>CVSS</b></td><td><b>4.0</b></td></tr>
<tr><td colspan="2"><b>Summary</b></td><td colspan="6">The remote service is using a SSLTLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.</td></tr>
<tr><td colspan="2"><b>Affected Nodes</b></td><td colspan="6">192.168.11.46 -</td></tr>
<tr><td colspan="2"><b>Impact</b></td><td colspan="6"></td></tr>
<tr><td colspan="2"><b>Solution</b></td><td colspan="4">Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.</td><td><b>Solution Type</b></td><td>Mitigation</td></tr>
<tr><td colspan="8"><b>Additional Details</b></td></tr>
<tr><td colspan="2"><b>CVE Description</b></td><td colspan="6">SSL/TLS: Certificate Signed Using A Weak Signature Algorithm</td></tr>
<tr><td colspan="2"><b>Detection Method</b></td><td colspan="6">Check which hashing algorithm was used to sign the remote SSL/TLS certificate.</td></tr>
<tr><td colspan="2"><b>Findings</b></td><td colspan="6">The following certificates are part of the certificate chain but using insecure signature algorithmsSubject 2.5.4.443616C69666F6D6961CUSLIrvineOCisco Systems Inc.OURV042CN78da6e650ddcSignature Algorithm sha1WithRSAEncryption</td></tr>
<tr><td colspan="2"><b>References</b></td><td colspan="6">https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/</td></tr>
</table>

<table>
<tr><th colspan="8">CVE-2020-20231</th></tr>
<tr><td>Risk</td><td>Medium</td><td></td><td>Threat Type</td><td>Denial of Service</td><td></td><td>CVSS</td><td>4.0</td></tr>
<tr><td colspan="2">Summary</td><td colspan="6">MikroTik RouterOS is prone to a denial of service DoS vulnerability.</td></tr>
<tr><td colspan="2">Affected Nodes</td><td colspan="6">192.168.11.62 -</td></tr>
<tr><td colspan="2">Impact</td><td colspan="6"></td></tr>
<tr><td colspan="2">Solution</td><td colspan="3">No known solution is available as of 11th March, 2022.   Information regarding this issue will be updated once solution details are available.</td><td colspan="2">Solution Type</td><td>NoneAvailable</td></tr>
<tr><td colspan="8">Additional Details</td></tr>
<tr><td colspan="2">CVE Description</td><td colspan="6">Mikrotik RouterOs through stable version 6.48.3 suffers from a memory corruption vulnerability in the /nova/bin/detnet process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference). MikroTik RouterOS <= 6.48.3 DoS Vulnerability</td></tr>
<tr><td colspan="2">Detection Method</td><td colspan="6">Checks if a vulnerable version is present on the target host.</td></tr>
<tr><td colspan="2">Findings</td><td colspan="6">Installed version 6.47.10Fixed version   None</td></tr>
<tr><td colspan="2">References</td><td colspan="6">https://github.com/cq674350529/pocs_slides/blob/master/advisory/MikroTik/CVE-2020-20231/README.md</td></tr>
</table>

CVE-2015-5174							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**4.0**
Summary	Apache Tomcat is prone to a limited directory traversal vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote authenticated users to bypass intended SecurityManager restrictions and list a parent directory.						
Solution	Upgrade to version 6.0.45 or 7.0.65 or 8.0.27 or later.				**Solution Type**	VendorFix	
Additional Details							
CVE Description	Directory traversal vulnerability in RequestUtil.java in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.65, and 8.x before 8.0.27 allows remote authenticated users to bypass intended SecurityManager restrictions and list a parent directory via a /.. (slash dot dot) in a pathname used by a web application in a getResource, getResourceAsStream, or getResourcePaths call, as demonstrated by the $CATALINA_BASE/webapps directory. Apache Tomcat Limited Directory Traversal Vulnerability - Feb16 (Windows)						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 6.0.45Installationpath port 8080tcp						
References	http://tomcat.apache.org/security-9.html http://www.securityfocus.com/bid/83329 http://tomcat.apache.org/security-8.html http://tomcat.apache.org/security-7.html http://tomcat.apache.org/security-6.html						

<table>
<tr><th colspan="8"></th></tr>
<tr><td><strong>Risk</strong></td><td><strong>Medium</strong></td><td></td><td><strong>Threat Type</strong></td><td>SSL and TLS</td><td></td><td><strong>CVSS</strong></td><td><strong>4.0</strong></td></tr>
<tr><td colspan="2"><strong>Summary</strong></td><td colspan="6">The SSLTLS service uses Diffie-Hellman groups with insufficient strength key size 2048.</td></tr>
<tr><td colspan="2"><strong>Affected Nodes</strong></td><td colspan="6">192.168.11.31 -</td></tr>
<tr><td colspan="2"><strong>Impact</strong></td><td colspan="6">An attacker might be able to decrypt the SSL/TLS communication offline.</td></tr>
<tr><td colspan="2"><strong>Solution</strong></td><td colspan="3">Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use   a 2048-bit or stronger Diffie-Hellman group (see the references).   For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.</td><td colspan="2"><strong>Solution Type</strong></td><td>Workaround</td></tr>
<tr><td colspan="8"><strong>Additional Details</strong></td></tr>
<tr><td colspan="2"><strong>CVE Description</strong></td><td colspan="6">SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability</td></tr>
<tr><td colspan="2"><strong>Detection Method</strong></td><td colspan="6">Checks the DHE temporary public key size.</td></tr>
<tr><td colspan="2"><strong>Findings</strong></td><td colspan="6">Server Temporary Key Size 1024 bits</td></tr>
<tr><td colspan="2"><strong>References</strong></td><td colspan="6">https://weakdh.org/
https://weakdh.org/sysadmin.html</td></tr>
</table>

CVE-2021-34428							
Risk	Medium		Threat Type	Web Servers		CVSS	3.6
Summary	Eclipse Jetty is prone to a vulnerability in the session management.						
Affected Nodes	192.168.11.226 -						
Impact							
Solution	Update to version 9.4.41.v20210516, 10.0.3, 11.0.3 or later.				Solution Type	VendorFix	
Additional Details							
CVE Description	For Eclipse Jetty versions &amp;lt;= 9.4.40, &amp;lt;= 10.0.2, &amp;lt;= 11.0.2, if an exception is thrown from the SessionListener#sessionDestroyed() method, then the session ID is not invalidated in the session ID manager. On deployments with clustered sessions and multiple contexts this can result in a session not being invalidated. This can result in an application used on a shared computer being left logged in. Eclipse Jetty Session Vulnerability (GHSA-m6cp-vxjx-65j6) - Windows						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 7.6.9.20130131Fixed version 9.4.41.20210516Installationpath port 6143tcp						
References	https://github.com/eclipse/jetty.project/security/advisories/GHSA-m6cp-vxjx-65j6						

CVE-2016-7463							
Risk	Medium		Threat Type	General		CVSS	3.5
Summary	VMware product updates address a critical glibc security vulnerability						
Affected Nodes	192.168.11.14 -						
Impact							
Solution	Apply the missing patch(es).				Solution Type	VendorFix	
Additional Details							
CVE Description	Cross-site scripting (XSS) vulnerability in the Host Client in VMware vSphere Hypervisor (aka ESXi) 5.5 and 6.0 allows remote authenticated users to inject arbitrary web script or HTML via a crafted VM. VMSA-2016-003: VMware ESXi updates address a cross-site scripting issue (remote check)						
Detection Method	Check the build number						
Findings	ESXi Version 6.0.0Detected Build 2494585Fixed Build 4558694						
References	http://www.vmware.com/security/advisories/VMSA-2016-0023.html						

Risk	**Medium**		**Threat Type**	General		**CVSS**	**2.6**
Summary	The remote host implements TCP timestamps and therefore allows to compute the uptime.						
Affected Nodes	192.168.11.4 -						
Impact	A side effect of this feature is that the uptime of the remote host can sometimes be computed.						
Solution	To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.					**Solution Type**	Mitigation
Additional Details							
CVE Description	TCP timestamps						
Detection Method	Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.						
Findings	It was detected that the host implements RFC1323RFC7323.The following timestamps were retrieved with a delay of 1 seconds in-betweenPacket 1 43917237Packet 2 43917250						
References	http://www.ietf.org/rfc/rfc1323.txt http://www.ietf.org/rfc/rfc7323.txt https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152						

CVE-2010-1157							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**2.6**
Summary	Apache Tomcat is prone to a remote information-disclosure vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Remote attackers can exploit this issue to obtain the host name or IP address of the Tomcat server. Information harvested may lead to further attacks.						
Solution	Updates are available. Please see the references for more information.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Apache Tomcat 5.5.0 through 5.5.29 and 6.0.0 through 6.0.26 might allow remote attackers to discover the server's hostname or IP address by sending a request for a resource that requires (1) BASIC or (2) DIGEST authentication, and then reading the realm field in the WWW-Authenticate header in the reply. Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability						
Detection Method							
Findings	Installed version 6.0.24Fixed version 5.5.306.0.27Installationpath port 8080tcp						
References	http://www.securityfocus.com/bid/39635 http://tomcat.apache.org/security-5.html http://tomcat.apache.org/security-6.html http://svn.apache.org/viewvc?view=revision&revision=936540 http://svn.apache.org/viewvc?view=revision&revision=936541 http://www.securityfocus.com/archive/1/510879						

Risk	**Medium**		**Threat Type**	General		**CVSS**	**2.6**
Summary	The remote host uses non-random IP IDs that is it is possible to predict the next value of the ipid field of the ip packets sent by this host.						
Affected Nodes	192.168.11.47 -						
Impact	An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are: 1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network. 2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines. 3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.						
Solution	Contact your vendor for a patch				**Solution Type**		VendorFix
Additional Details							
CVE Description	Relative IP Identification number change						
Detection Method							
Findings	The target host was found to be vulnerable						
References							

CVE-2010-1157							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**2.6**
Summary	Apache Tomcat server is prone to a security bypass vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Remote attackers can exploit this issue to obtain the host name or IP address of the Tomcat server. Information harvested may aid in further attacks.						
Solution	Upgrade to the latest version of Apache Tomcat 5.5.30 or 6.0.27 or later.				**Solution Type**		VendorFix
Additional Details							
CVE Description	Apache Tomcat 5.5.0 through 5.5.29 and 6.0.0 through 6.0.26 might allow remote attackers to discover the server's hostname or IP address by sending a request for a resource that requires (1) BASIC or (2) DIGEST authentication, and then reading the realm field in the WWW-Authenticate header in the reply. Apache Tomcat Security bypass vulnerability						
Detection Method							
Findings	Installed version 6.0.24Fixed version 5.5.306.0.27Installationpath port 8080tcp						
References	http://tomcat.apache.org/security-5.html http://tomcat.apache.org/security-6.html http://www.securityfocus.com/archive/1/510879						

Risk	**Medium**		**Threat Type**	General		**CVSS**	**2.6**
Summary	The remote SSH server is configured to allow support weak MAC algorithms.						
Affected Nodes	192.168.11.22 -						
Impact							
Solution	Disable the reported weak MAC algorithm(s).				**Solution Type**		Mitigation
Additional Details							
CVE Description	Weak MAC Algorithm(s) Supported (SSH)						
Detection Method	Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server. Currently weak MAC algorithms are defined as the following: - MD5 based algorithms - 96-bit based algorithms - none algorithm						
Findings	The remote SSH server supports the following weak client-to-server MAC algorithmshmac-md5hmac-sha1-96The remote SSH server supports the following weak server-to-client MAC algorithmshmac-md5hmac-sha1-96						
References							

CVE-2017-11747							
Risk	Medium		Threat Type	Web application abuses		CVSS	2.1
Summary	Tinyproxy creates a runtinyproxytinyproxy.pid file after dropping privileges to a non-root account which might allow local users to kill arbitrary processes by leveraging access to this non-root account for tinyproxy.pid modification before a root script executes a kill command.						
Affected Nodes	192.168.13.48 -						
Impact							
Solution	Update Tinyproxy to version 1.10.0 or later.				Solution Type	VendorFix	
Additional Details							
CVE Description	Main.c in Tinyproxy 1.8.4 and earlier creates a /run/tinyproxy/tinyproxy.pid file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for tinyproxy.pid modification before a root script executes a "kill `cat /run/tinyproxy/tinyproxy.pid`" command. Tinyproxy DoS Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 1.8.2Fixed version 1.10.0						
References	https://github.com/tinyproxy/tinyproxy/releases/tag/1.10.0 https://github.com/tinyproxy/tinyproxy/issues/106						

CVE-2011-2204							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**1.9**
Summary	Apache Tomcat is prone to a remote information-disclosure vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Remote attackers can exploit this issue to obtain sensitive information that will aid in further attacks.						
Solution	Updates are available. Please see the references for more information.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.17, when the MemoryUserDatabase is used, creates log entries containing passwords upon encountering errors in JMX user creation, which allows local users to obtain sensitive information by reading a log file. Apache Tomcat 'MemoryUserDatabase' Information Disclosure Vulnerability						
Detection Method							
Findings	Installed version 6.0.24Fixed version 5.5.346.0.337.0.17Installationpath port 8080tcp						
References	http://www.securityfocus.com/bid/48456 http://tomcat.apache.org/security-5.html http://tomcat.apache.org/security-6.html http://tomcat.apache.org/security-7.html http://support.avaya.com/css/P8/documents/100147910						

CVE-2010-3718							
Risk	**Medium**		**Threat Type**	Web Servers		**CVSS**	**1.2**
Summary	Apache Tomcat is prone to a security bypass vulnerability.						
Affected Nodes	192.168.11.86 -						
Impact	Successful exploitation will allow remote attackers to bypass certain authentication and obtain sensitive information.						
Solution	Upgrade Apache Tomcat version to 5.5.30, 6.0.30, 7.0.4 or later.					**Solution Type**	VendorFix
Additional Details							
CVE Description	Apache Tomcat 7.0.0 through 7.0.3, 6.0.x, and 5.5.x, when running within a SecurityManager, does not make the ServletContext attribute read-only, which allows local web applications to read or write files outside of the intended working directory, as demonstrated using a directory traversal attack. Apache Tomcat SecurityManager Security Bypass Vulnerability						
Detection Method	Checks if a vulnerable version is present on the target host.						
Findings	Installed version 6.0.24Fixed version 5.5.306.0.307.0.4Installationpath port 8080tcp						
References	http://xforce.iss.net/xforce/xfdb/65159 http://www.securitytracker.com/id?1025025						