VONAHI SECURITY

Monthly Internal network scan

VULNERABILITY REPORT

Infowerks Data Services

November 15, 2025

Copyright

The methodology used to audit the computer systems is considered proprietary intellectual information of Vonahi Security and may not be disclosed without written permission from Vonahi Security. Vonahi Security gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Alton Johnson
Title:	Principal Security Consultant
Office:	(844) 866-2732
Email:	support@vpentest.io

Discovered Vulnerabilities

The following table displays a summary of the vulnerabilities that were discovered as part of this engagement.

DISCOVERED VULNERABILITIES	THREAT SEVERITY RANKINGS	
Internal Vulnerability Assessment (142)		
7-Zip Multiple Vulnerabilities - Windows	Critical	▮▮▮▮▮
7-Zip RCE Vulnerability - Windows	Critical	▮▮▮▮▮
Adobe Flash Player End of Life (EOL) Detection	Critical	▮▮▮▮▮
Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-19) - Windows	Critical	▮▮▮▮▮
Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-46) - Windows	Critical	▮▮▮▮▮
Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB20-30) - Windows	Critical	▮▮▮▮▮
Apache Struts Security Update (S2-045) - Active Check	Critical	▮▮▮▮▮
Apache Tomcat 'CORS Filter' Setting Security Bypass Vulnerability	Critical	▮▮▮▮▮
Apache Tomcat End of Life (EOL) Detection - Windows	Critical	▮▮▮▮▮
Apache Tomcat Multiple Vulnerabilities (Feb 2020) - Windows	Critical	▮▮▮▮▮
Apache Tomcat RCE Vulnerability (Mar 2025) - Windows	Critical	▮▮▮▮▮
Apache Tomcat Rewrite Rule Bypass Vulnerability (Apr 2025) - Windows	Critical	▮▮▮▮▮
CUPS Multiple Vulnerabilities (Sep/Oct 2024)	Critical	▮▮▮▮▮
.NET Core Multiple Vulnerabilities (KB5033734)	Critical	▮▮▮▮▮
.NET Core Multiple Vulnerabilities (Oct 2025)	Critical	▮▮▮▮▮
.NET Core Multiple Vulnerabilities - Windows	Critical	▮▮▮▮▮
7zip Authentication Bypass Vulnerability - Windows	High	▮▮▮▮▯
7-Zip Mark-of-the-Web Bypass Vulnerability (Jan 2025) - Windows	High	▮▮▮▮▯
7-Zip Multiple Vulnerabilities (Jul 2025) - Windows	High	▮▮▮▮▯
7-Zip Qcow Handler Infinite Loop DoS Vulnerability - Windows	High	▮▮▮▮▯
7zip RAR Denial of Service Vulnerability - Windows	High	▮▮▮▮▯
7Zip UDF CInArchive::ReadFileItem Code Execution Vulnerability	High	▮▮▮▮▯
7-Zip Zstandard Decompression Integer Underflow Vulnerability - Windows	High	▮▮▮▮▯

Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-26) - Windows	High	📶
Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-30) - Windows	High	📶
Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB20-06) - Windows	High	📶
Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB20-58) - Windows	High	📶
Apache Tomcat Clustering DoS Vulnerability (May 2022)	High	📶
Apache Tomcat DoS Vulnerability (Feb 2023) - Windows	High	📶
Apache Tomcat DoS Vulnerability (Jul 2024) - Windows	High	📶
Apache Tomcat DoS Vulnerability (Jul 2025) - Windows	High	📶
Apache Tomcat DoS Vulnerability (Jun 2019) - Windows	High	📶
Apache Tomcat DoS Vulnerability (Jun 2020) - Windows	High	📶
Apache Tomcat DoS Vulnerability (Mar 2019) - Windows	High	📶
Apache Tomcat DoS Vulnerability (Oct 2021) - Windows	High	📶
Apache Tomcat DoS Vulnerability (Sep 2021) - Windows	High	📶
Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows	High	📶
Apache Tomcat HTTP/2 Protocol DoS Vulnerability (MadeYouReset) - Windows	High	📶
Apache Tomcat HTTP/2 Vulnerability (Dec 2020) - Windows	High	📶
Apache Tomcat Information Disclosure Vulnerability (Mar 2021) - Windows	High	📶
Apache Tomcat Local Privilege Escalation Vulnerability (Jan 2022) - Windows	High	📶
Apache Tomcat Multiple DoS Vulnerabilities (Jul 2020) - Windows	High	📶
Apache Tomcat Multiple DoS Vulnerabilities (Jul 2025) - Windows	High	📶
Apache Tomcat Multiple Vulnerabilities (Jun 2025) - Windows	High	📶
Apache Tomcat Multiple Vulnerabilities (Oct 2023) - Windows	High	📶
Apache Tomcat Privilege Escalation Vulnerability (Dec 2019) - Windows	High	📶
Apache Tomcat RCE Vulnerability (Apr 2019) - Windows	High	📶
Apache Tomcat RCE Vulnerability (Mar 2021) - Windows	High	📶
Apache Tomcat RCE Vulnerability (May 2020) - Windows	High	📶
Apache Tomcat Request Mix-up Vulnerability (May 2022) - Windows	High	📶
Apache Tomcat Request Smuggling Vulnerability (Nov 2023) - Windows	High	📶

Apache Tomcat Request Smuggling Vulnerability (Oct 2022) - Windows	High	📶
Apache Tomcat Session Fixation Vulnerability (Aug 2025) - Windows	High	📶
Apache Tomcat Session Fixation Vulnerability (Dec 2019) - Windows	High	📶
CUPS 2.4.7 Buffer Overflow Vulnerability	High	📶
Dell DRAC / iDRAC Default Credentials (HTTP)	High	📶
Deprecated SSH-1 Protocol Detection	High	📶
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)	High	📶
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)	High	📶
.NET Core Denial of Service And Information Disclosure Vulnerabilities - Windows	High	📶
.NET Core Denial of Service Vulnerability - Windows	High	📶
.NET Core DoS Vulnerability (Feb 2024) - Windows	High	📶
.NET Core DoS Vulnerability (May 2020)	High	📶
.NET Core Elevation of Privilege Vulnerability (Mar 2025)	High	📶
.NET Core Multiple Denial of Service Vulnerabilities (KB5014326)	High	📶
.NET Core Multiple Denial of Service Vulnerabilities (KB5036452)	High	📶
.NET Core Multiple DoS Vulnerabilities-01 (May 2019)	High	📶
.NET Core Multiple DoS Vulnerabilities-02 (May 2019)	High	📶
.NET Core Multiple DoS Vulnerabilities - Windows	High	📶
.NET Core Multiple Vulnerabilities (KB5041081)	High	📶
.NET Core Multiple Vulnerabilities (KB5042132)	High	📶
.NET Core Multiple Vulnerabilities (KB5045993)	High	📶
.NET Core Multiple Vulnerabilities (Sep 2019)	High	📶
.NET Core OData Denial of Service Vulnerability - Windows	High	📶
.NET Core Privilege Escalation Vulnerability (KB5037337)	High	📶
.NET Core Privilege Escalation Vulnerability (KB5037338)	High	📶
.NET Core RCE Vulnerability (Jan 2025)	High	📶
.NET Core RCE Vulnerability (January-1 2025)	High	📶
.NET Core RCE Vulnerability (Jun 2025)	High	📶

.NET Core Remote Code Execution Vulnerability - Windows	High	▮▮▮▮▯
.NET Core SDK DoS Vulnerability (May 2020)	High	▮▮▮▮▯
.NET Core SDK Multiple DoS Vulnerabilities-01 (May 2019)	High	▮▮▮▮▯
.NET Core SDK Multiple DoS Vulnerabilities-02 (May 2019)	High	▮▮▮▮▯
.NET Core SDK Multiple Vulnerabilities (Sep 2019)	High	▮▮▮▮▯
.NET Core SDK Security Feature Bypass Vulnerability (Sep 2020)	High	▮▮▮▮▯
.NET Core Security Feature Bypass Vulnerability (Sep 2020)	High	▮▮▮▮▯
.NET Core Spoofing Vulnerability (May 2025)	High	▮▮▮▮▯
Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-06) - Windows	Medium	▮▮▮▯▯
Apache Tomcat Authentication Bypass Vulnerability (Nov 2024) - Windows	Medium	▮▮▮▯▯
Apache Tomcat CGI Security Constraint Bypass Vulnerability (May 2025) - Windows	Medium	▮▮▮▯▯
Apache Tomcat HTTP/2 Vulnerability (Oct 2020) - Windows	Medium	▮▮▮▯▯
Apache Tomcat HTTP Request Smuggling Vulnerability (Jul 2021) - Windows	Medium	▮▮▮▯▯
Apache Tomcat Information Disclosure Vulnerability (Jan 2021) - Windows	Medium	▮▮▮▯▯
Apache Tomcat Information Disclosure Vulnerability (Jan 2024) - Windows	Medium	▮▮▮▯▯
Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows	Medium	▮▮▮▯▯
Apache Tomcat JNDI Realm Authentication Weakness Vulnerability (Jul 2021) - Windows	Medium	▮▮▮▯▯
Apache Tomcat Multiple DoS Vulnerabilities (Mar 2024) - Windows	Medium	▮▮▮▯▯
Apache Tomcat Multiple Vulnerabilities (Dec 2024) - Windows	Medium	▮▮▮▯▯
Apache Tomcat 'NIO/NIO2' Connectors Information Disclosure Vulnerability - Windows	Medium	▮▮▮▯▯
Apache Tomcat Open Redirect Vulnerability (Aug 2023) - Windows	Medium	▮▮▮▯▯
Apache Tomcat Open Redirect Vulnerability - Windows	Medium	▮▮▮▯▯
Apache Tomcat XSS Vulnerability (Jun 2022) - Windows	Medium	▮▮▮▯▯
Apache Tomcat XSS Vulnerability (May 2019) - Windows	Medium	▮▮▮▯▯
AppleShare IP / Apple Filing Protocol (AFP) Unencrypted Cleartext Login	Medium	▮▮▮▯▯
Backup File Scanner (HTTP) - Unreliable Detection Reporting	Medium	▮▮▮▯▯
Cleartext Transmission of Sensitive Information via HTTP	Medium	▮▮▮▯▯
CUPS 2.4.13 Multiple Vulnerabilities	Medium	▮▮▮▯▯

CUPS 2.4.3 DoS Vulnerability	Medium	📶
CUPS 2.4.9 File Permission Vulnerability	Medium	📶
DCE/RPC and MSRPC Services Enumeration Reporting	Medium	📶
Dell OpenManage Server Administrator Directory Traversal Vulnerability (Apr 2016)	Medium	📶
.NET Core Denial of Service Vulnerability (Jun 2021)	Medium	📶
.NET Core Information Disclosure Vulnerabilities - Windows	Medium	📶
.NET Core Information Disclosure Vulnerability (KB5015424)	Medium	📶
.NET Core Multiple Vulnerabilities (KB5038351)	Medium	📶
.NET Core SDK Spoofing Vulnerability (Feb 2019)	Medium	📶
.NET Core SDK Spoofing Vulnerability (Jul 2019)	Medium	📶
.NET Core Spoofing Vulnerability (Feb 2019)	Medium	📶
.NET Core Spoofing Vulnerability (Jul 2019)	Medium	📶
7-Zip Arbitrary File Write Vulnerability (Oct 2025) - Windows	Low	📶
7-Zip Multiple Vulnerabilities (Apr 2025) - Windows	Low	📶
Apache Tomcat Information Disclosure Vulnerability (Sep 2022) - Windows	Low	📶
7zip Detection (Windows SMB Login)	Informational	📶
Adobe Flash Player Within Microsoft IE and Edge Detection (Windows SMB Login)	Informational	📶
Adobe Products Detection (Windows SMB Login)	Informational	📶
Allowed HTTP Methods Enumeration	Informational	📶
Anti-Scanner Defenses (HTTP)	Informational	📶
AnyDesk Desktop Detection Consolidation	Informational	📶
Apache HTTP Server Detection Consolidation	Informational	📶
Apache Tomcat Detection Consolidation	Informational	📶
Apple / OpenPrinting CUPS Detection (HTTP)	Informational	📶
AppleShare IP / Apple Filing Protocol (AFP) Service Detection	Informational	📶
ASP.NET Core/.NET Core SDK Detection (Windows SMB Login)	Informational	📶
Authenticated Scan / LSC Info Consolidation (Windows SMB Login)	Informational	📶
BIOS and Hardware Information Detection (Windows SMB Login)	Informational	📶

Check for Windows 10 Cortana Search	Informational	▮▯▯▯▯
Compatibility Issues Affecting Signed Microsoft Binaries (2749655)	Informational	▮▯▯▯▯
Cygwin Detection (Windows SMB Login)	Informational	▮▯▯▯▯
DCE/RPC and MSRPC Services Enumeration	Informational	▮▯▯▯▯
Dell DRAC / iDRAC Detection Consolidation	Informational	▮▯▯▯▯
Dell EMC OpenManage Server Administrator (OMSA) Detection (HTTP)	Informational	▮▯▯▯▯
'favicon.ico' Based Fingerprinting (HTTP)	Informational	▮▯▯▯▯

Vulnerability Findings

This section of the report contains all of the vulnerabilities that were discovered for each component conducted throughout the vulnerability assessment.

Internal Vulnerability Assessment

Engagement Scope of Work

Through discussions with Infowerks's staff, the following target applications, IP addresses, and/or ranges were included as part of the engagement scope.

IP ADDRESSES & RANGES			
192.168.100.0/23	192.168.199.0/24		

7-Zip Multiple Vulnerabilities - Windows	
Severity	📶
Description	7zip is prone to multiple vulnerabilities. Insight: These vulnerabilities exist: - CVE-2023-52168: A heap-based overflow vulnerability - CVE-2023-52169: An out-of-bounds read vulnerability. Affected systems: 7zip version prior to 24.01 on Windows. Impact: Successful exploitation allows an attacker to overwrite two bytes at multiple offsets beyond the allocated buffer size and to read beyond the intended buffer.
Recommendation	Update to version 24.01.
References	Cve: CVE-2023-52168 Cve: CVE-2023-52169 Url: https://www.openwall.com/lists/oss-security/2024/07/03/10 Cert-bund: WID-SEC-2024-1516
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 9.20`
	`Fixed version:     24.01`
	`Installation`
	`path / port:       Unable to find the install location`

7-Zip RCE Vulnerability - Windows	
Severity	📶
Description	7zip is prone to a remote code execution (RCE) vulnerability. Insight: The flaw exists due to an out-of-bounds write error in 7zip. Affected systems: 7zip version prior to 23.00 on Windows. Impact: Successful exploitation allows an attacker to execute arbitrary code.
Recommendation	Update to version 23.00.
References	Cve: CVE-2023-40481 Url: https://sourceforge.net/p/sevenzip/patches/417/ Cert-bund: WID-SEC-2023-2183
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 9.20`
	`Fixed version:     23.00`
	`Installation`
	`path / port:       Unable to find the install location`

Adobe Flash Player End of Life (EOL) Detection	
Severity	📶
Description	The Adobe Flash Player on the remote host has reached the end of life (EOL) / is discontinued and should not be used anymore.

	Impact: An EOL / discontinued product 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.
Recommendation	No solution was made available by the vendor. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. Note: The product has reached its EOL.
References	Url: https://www.adobe.com/products/flashplayer/end-of-life.html Url: https://theblog.adobe.com/adobe-flash-update/
Affected Nodes	192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.192 (ILAS3DB160.infowerks.com) on port 0/tcp 192.168.101.184 (ilas3db140.infowerks.com) on port 0/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.101.185 (ilas3stor01.infowerks.com) on port 0/tcp

Additional Output	`The "Adobe Flash Player" product on the remote host has reached the end of life.`
	
	`CPE:            cpe:/a:adobe:flash_player_internet_explorer`
	`Location/URL:   C:\Windows\SysWOW64`
	`EOL date:       2020-12-31`
	`EOL info:       https://www.adobe.com/products/flashplayer/end-of-life.html`

Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-19) - Windows

Severity	▮▮▮▮▮
Description	Adobe Flash Player within Microsoft Edge or Internet Explorer is prone to a remote code execution (RCE) vulnerability. Insight: Multiple flaws are due to: - An out of bounds read error. - An use after free error. Affected systems: Adobe Flash Player prior to 32.0.0.171 within Microsoft Edge or Internet Explorer on, Windows 10 Version 1607 for x32/x64 Edition, Windows 10 Version 1703 for x32/x64 Edition, Windows 10 Version 1709 for x32/x64 Edition, Windows 10 Version 1803 for x32/x64 Edition, Windows 10 Version 1809 for x32/x64 Edition, Windows 10 x32/x64 Edition, Windows 8.1 for x32/x64 Edition, Windows Server 2012/2012 R2, Windows Server 2016 Impact: Successful exploitation allows attackers to disclose sensitive information and execute arbitrary code.

CVSS3	9.8
Recommendation	Upgrade to Adobe Flash Player 32.0.0.171 or later. Please see the references for more information.
References	Cve: CVE-2019-7096 Cve: CVE-2019-7108 Url: https://helpx.adobe.com/security/products/flash-player/apsb19-19.html Cert-bund: CB-K19/0299
Affected Nodes	192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp

Additional Output	`Vulnerable range:  Less than 32.0.0.171`
	`File checked:      C:\Windows\SysWOW64\Flashplayerapp.exe`
	`File version:      11.8.800.133`

Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-46) - Windows

Severity	▂▃▅▆█
Description	Adobe Flash Player is prone to multiple vulnerabilities. Insight: Multiple flaws exist due to: - An use after free vulnerability. - Same Origin Method Execution (SOME) Vulnerability. Affected systems: Adobe Flash Player prior to 32.0.0.255 within Microsoft Edge or Internet Explorer on, Windows 10 Version 1607 for x32/x64 Edition, Windows 10 Version 1703 for x32/x64 Edition, Windows 10 Version 1709 for x32/x64 Edition, Windows 10 Version 1803 for x32/x64 Edition, Windows 10 Version 1809 for x32/x64 Edition, Windows 10 Version 1903 for x32/x64 Edition, Windows 10 x32/x64 Edition, Windows 8.1 for x32/x64 Edition, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 Impact: Successful exploitation allows attackers to conduct arbitrary code execution.
CVSS3	9.8
Recommendation	Upgrade to Adobe Flash Player 32.0.0.255 or later. Please see the references for more information.
References	Cve: CVE-2019-8070 Cve: CVE-2019-8069 Url: https://helpx.adobe.com/security/products/flash-player/apsb19-46.html Cert-bund: CB-K19/0800
Affected Nodes	192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp

Additional Output	`Vulnerable range:  Less than 32.0.0.255`
	`File checked:      C:\Windows\SysWOW64\Flashplayerapp.exe`
	`File version:      11.8.800.133`

Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB20-30) - Windows

Severity	▂▃▅▆▇
Description	Adobe Flash Player is prone to an arbitrary code execution vulnerability. Insight: The flaw exists due to a use-after-free error. Affected systems: Adobe Flash Player prior to 32.0.0.387 within Microsoft Edge or Internet Explorer on: Windows 10 Version 1607 for x32/x64 Edition Windows 10 Version 1703 for x32/x64 Edition Windows 10 Version 1709 for x32/x64 Edition Windows 10 Version 1803 for x32/x64 Edition Windows 10 Version 1809 for x32/x64 Edition Windows 10 Version 1903 for x32/x64 Edition Windows 10 Version 1909 for x32/x64 Edition Windows 10 Version 2004 for x32/x64 Edition Windows 10 x32/x64 Edition Windows 8.1 for x32/x64 Edition Windows Server 2012/2012 R2 Windows Server 2016 Windows Server 2019 Impact: Successful exploitation allows attackers to execute arbitrary code.
CVSS3	9.8
Recommendation	Update to Adobe Flash Player 32.0.0.387 or later.
References	Cve: CVE-2020-9633 Url: https://helpx.adobe.com/security/products/flash-player/apsb20-30.html Cert-bund: CB-K20/0566
Affected Nodes	192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.184 (ilas3db140.infowerks.com) on port 0/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.101.185 (ilas3stor01.infowerks.com) on port 0/tcp

Additional Output	`Vulnerable range:  Less than 32.0.0.387`
	`File checked:      C:\Windows\SysWOW64\Flashplayerapp.exe`
	`File version:      32.0.0.330`

Apache Struts Security Update (S2-045) - Active Check

Severity	▂▃▅▆▇
Description	Apache Struts is prone to a remote code execution (RCE) vulnerability. Affected systems: Apache Struts 2.3.5 through 2.3.31 and 2.5 through 2.5.10. Impact: Successfully exploiting this issue may allow an attacker to execute arbitrary code in the context of the affected application.
CVSS3	9.8
Recommendation	Updates are available. Please see the referenced vendor advisory for more information.
References	Cve: CVE-2017-5638 Url: https://cwiki.apache.org/confluence/display/WW/S2-045 Advisory-id: S2-045 Url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog Cisa: Known Exploited Vulnerability (KEV) catalog Cert-bund: WID-SEC-2024-1277 Cert-bund: WID-SEC-2023-0461 Cert-bund: CB-K17/1198 Cert-bund: CB-K17/0661 Cert-bund: CB-K17/0657 Cert-bund: CB-K17/0402
Affected Nodes	192.168.101.221 (ilas1as09.infowerks.com) on port 443/tcp

Additional Output

```
It was possible to execute the command `ipconfig` on the remote host.

Request:

POST /statsreport/ HTTP/1.1
Host: ilas1as09
Pragma: no-cache
User-Agent: Mozilla/5.0 [en] (X11, U; OpenVAS-VT 23.20.1)
Accept-Language: en
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept: */*
Accept-Encoding: identity
Content-Length: 163
Content-Type:: %{(#OpenVASVT='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_
memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.contai
ner']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.ge
tExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#
dm)))).(#p=new java.lang.ProcessBuilder({'ipconfig'})).(#p.redirectErrorStream(true)).(#process=#p.st
art()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apach
e.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush(
------------ snipped ------------
```

Apache Tomcat 'CORS Filter' Setting Security Bypass Vulnerability

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to a security bypass vulnerability. Insight: The flaw exists because defaults settings for the CORS filter provided in Apache Tomcat are insecure and enable 'supportsCredentials' for all origins. Affected systems: Apache Tomcat versions 9.0.0.M1 to 9.0.8 Apache Tomcat versions 8.5.0 to 8.5.31 Apache Tomcat versions 8.0.RC1 to 8.0.52 Apache Tomcat versions 7.0.41 to 7.0.88 Impact: Successful exploitation will allow remote

	attackers to bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks.
CVSS3	9.8
Recommendation	Upgrade to Apache Tomcat version 9.0.9, 8.0.53, 7.0.89 or 8.5.32 or later. Please see the references for more information.
References	Cve: CVE-2018-8014 Url: http://tomcat.apache.org/security-9.html Url: http://www.securityfocus.com/bid/104203 Url: http://tomcat.apache.org/security-8.html Url: http://tomcat.apache.org/security-7.html Cert-bund: WID-SEC-2024-0528 Cert-bund: CB-K18/1005 Cert-bund: CB-K18/0680
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.9`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat End of Life (EOL) Detection - Windows	
Severity	▂▃▅▆▇
Description	The Apache Tomcat version on the remote host has reached the end of life (EOL) and should not be used anymore. 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.
Recommendation	Update the Apache Tomcat version on the remote host to a still supported version.
References	Url: https://tomcat.apache.org/tomcat-10.0-eol.html Url: https://tomcat.apache.org/tomcat-85-eol.html Url: https://tomcat.apache.org/tomcat-80-eol.html Url: https://tomcat.apache.org/tomcat-70-eol.html Url: https://tomcat.apache.org/tomcat-60-eol.html Url: https://tomcat.apache.org/tomcat-55-eol.html Url: https://en.wikipedia.org/wiki/Apache_Tomcat#Releases Url: https://tomcat.apache.org/whichversion.html
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`The "Apache Tomcat" version on the remote host has reached the end of life.`
	
	`CPE:               cpe:/a:apache:tomcat:8.5.71`
	`Installed version: 8.5.71`
	`Location/URL:      9443/tcp`
	`EOL version:       8.5`
	`EOL date:          2024-03-31`

Apache Tomcat Multiple Vulnerabilities (Feb 2020) - Windows	
Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to multiple vulnerabilities. Insight: Apache Tomcat is prone to multiple vulnerabilities: - HTTP request smuggling vulnerability (CVE-2020-1935) - AJP Request Injection and potential Remote Code Execution dubbed 'Ghostcat' (CVE-2020-1938)

	Affected systems: Apache Tomcat 7.0.0 to 7.0.99, 8.5.0 to 8.5.50 and 9.0.0.M1 to 9.0.30.
CVSS3	9.8
Recommendation	Update to version 7.0.100, 8.5.51, 9.0.31 or later.
References	Cve: CVE-2020-1935 Cve: CVE-2020-1938 Cisa: Known Exploited Vulnerability (KEV) catalog Url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog Url: https://lists.apache.org/thread.html/r127f76181aceffea2bd4711b03c595d0f115f63e020348fe925a916c%40%3Cannounce.tomcat.apache.org%3E Url: https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E Url: https://www.chaitin.cn/en/ghostcat Url: https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487 Url: https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi Url: https://tomcat.apache.org/tomcat-7.0-doc/changelog.html Url: https://tomcat.apache.org/tomcat-8.5-doc/changelog.html Url: https://tomcat.apache.org/tomcat-9.0-doc/changelog.html Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2023-2480 Cert-bund: WID-SEC-2023-2130 Cert-bund: CB-K20/0711 Cert-bund: CB-K20/0705 Cert-bund: CB-K20/0693 Cert-bund: CB-K20/0555 Cert-bund: CB-K20/0543 Cert-bund: CB-K20/0165 Cert-bund: CB-K20/0154
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.31`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat RCE Vulnerability (Mar 2025) - Windows	
Severity	▁▂▃▅▇
Description	Apache Tomcat is prone to a remote code execution (RCE) vulnerability. Insight: The original implementation of partial PUT used a temporary file based on the user provided file name and path with the path separator replaced by '.'. If all of the following are true, a malicious user is able to view security sensitive files and/or inject content into those files: - writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - a target URL for security sensitive uploads that is a sub-directory of a target URL for public uploads - attacker knowledge of the names of security sensitive files being uploaded - the security sensitive files also being uploaded via partial PUT If all of the following are true, a malicious user is able to perform remote code execution:

	- writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - application is using Tomcat's file based session persistence with the default storage location - application includes a library that may be leveraged in a deserialization attack Affected systems: Apache Tomcat version 9.0.98 and prior, 10.x through 10.1.34 and 11.0.0-M1 through 11.0.2. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
CVSS3	9.8
Recommendation	Update to version 9.0.99, 10.1.35, 11.0.3 or later.
References	Cve: CVE-2025-24813 Cisa: Known Exploited Vulnerability (KEV) catalog Url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog Url: https://lists.apache.org/thread/j5fkjv2k477os90nczf2v9l61fb0kkgq Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.3 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.35 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.99 Url: https://github.com/iSee857/CVE-2025-24813-PoC Url: https://lab.wallarm.com/one-put-request-to-own-tomcat-cve-2025-24813-rce-is-in-the-wild/ Url: https://www.openwall.com/lists/oss-security/2025/03/10/5 Url: https://scrapco.de/blog/analysis-of-cve-2025-24813-apache-tomcat-path-equivalence-rce.html Url: https://bishopfox.com/blog/tomcat-cve-2025-24813-what-you-need-to-know-blog Cert-bund: WID-SEC-2025-1564 Cert-bund: WID-SEC-2025-1439 Cert-bund: WID-SEC-2025-0825 Cert-bund: WID-SEC-2025-0824 Cert-bund: WID-SEC-2025-0823 Cert-bund: WID-SEC-2025-0511
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.99`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat Rewrite Rule Bypass Vulnerability (Apr 2025) - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to a rewrite rule bypass vulnerability. Insight: For a subset of unlikely rewrite rule configurations, it is possible for a specially crafted request to bypass some rewrite rules. If those rewrite rules effectively enforced security constraints, those constraints could be bypassed. Affected systems: Apache Tomcat version 9.0.102 and prior, 10.x through 10.1.39 and 11.0.0-M1 through 11.0.5. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
CVSS3	9.8

Recommendation	Update to version 9.0.104, 10.1.40, 11.0.6 or later.
References	Cve: CVE-2025-31651 Url: https://lists.apache.org/thread/cpklvqwvdrp4k9hmd2l3q33j0gzy4fox Cert-bund: WID-SEC-2025-2372 Cert-bund: WID-SEC-2025-1850 Cert-bund: WID-SEC-2025-1572 Cert-bund: WID-SEC-2025-1565 Cert-bund: WID-SEC-2025-1563 Cert-bund: WID-SEC-2025-1439 Cert-bund: WID-SEC-2025-1365 Cert-bund: WID-SEC-2025-0895
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.104`
	`Installation`
	`path / port:       9443/tcp`

CUPS Multiple Vulnerabilities (Sep/Oct 2024)

Severity	▁▂▃▄▅
Description	Various components of CUPS are prone to multiple vulnerabilities. Insight: The following flaws exist: - CVE-2024-47076: cfGetPrinterAttributes5 does not validate IPP attributes returned from an IPP server (libcupsfilters) - CVE-2024-47175: ppdCreatePPDFromIPP2 does not sanitize IPP attributes when creating the PPD buffer (libppd) - CVE-2024-47176: Multiple bugs leading to info leak and remote code execution (cups-browsed) - CVE-2024-47850: Distributed denial-of-service (DDoS) attacks (cups-browsed) Affected systems: All CUPS systems which have the affected component(s) installed. Impact: Various flaws chained together could allow a remote code execution (RCE) on the affected host.
CVSS3	9.8
Recommendation	The vendor of cups-filters has provided fix commits: - libcupsfilters / CVE-2024-47076: Commit 95576ec - libppd / CVE-2024-47175: Commit d681747 - cups-browsed / CVE-2024-47176, CVE-2024-47850: Commit 1d1072a
References	Cve: CVE-2024-47076 Cve: CVE-2024-47175 Cve: CVE-2024-47176 Cve: CVE-2024-47850 Url: https://openprinting.github.io/libcupsfilters,-libppd,-cups-filters-2.1.0-Releases-including-vulnerability-fix/ Url: https://www.evilsocket.net/2024/09/26/Attacking-UNIX-systems-via-CUPS-Part-I/ Url: https://openprinting.github.io/OpenPrinting-News-Flash-cups-browsed-Remote-Code-Execution-vulnerability/ Url: https://isc.sans.edu/diary/Patch+for+Critical+CUPS+vulnerability+Dont+Panic/31302 Url: https://www.openwall.com/lists/oss-security/2024/09/26/5 Url: https://gist.github.com/stong/c8847ef27910ae344a7b5408d9840ee1 Url: https://access.redhat.com/security/vulnerabilities/RHSB-2024-002

	Url: https://github.com/OpenPrinting/cups-browsed/security/advisories/GHSA-rj88-6mr5-rcw8 Url: https://github.com/OpenPrinting/libcupsfilters/security/advisories/GHSA-w63j-6g73-wmg5 Url: https://github.com/OpenPrinting/libppd/security/advisories/GHSA-7xfx-47qg-grp6 Url: https://github.com/OpenPrinting/cups-filters/security/advisories/GHSA-p9rh-jxmq-gq47 Url: https://github.com/RickdeJager/cupshax Url: https://www.akamai.com/blog/security-research/october-cups-ddos-threat Cert-bund: WID-SEC-2024-3069 Cert-bund: WID-SEC-2024-2240
Affected Nodes	192.168.101.200 on port 631/tcp

Additional Output	`Installed version: 2.1`
	`Fixed version:     None`

.NET Core Multiple Vulnerabilities (KB5033734)

Severity	▂▃▅▆▇
Description	This host is missing an important security update according to Microsoft KB5033734. Insight: Multiple flaws exist due to, - Microsoft Identity Denial of service vulnerability. - Microsoft.Data.SqlClient and System.Data.SqlClient SQL Data Provider Security Feature Bypass Vulnerability. - NET, .NET Framework, and Visual Studio Security Feature Bypass Vulnerability. - .NET Denial of Service Vulnerability. Affected systems: .NET Core runtime 7.0 before 7.0.15 and .NET Core SDK before 7.0.405. Impact: Successful exploitation will allow an attacker to conduct denial of service and secuirity feature bypass on an affected system.
CVSS3	9.8
Recommendation	Upgrade .NET Core runtime to version 7.0.15 or later or upgrade .NET Core SDK to version 7.0.405 or later.
References	Cve: CVE-2024-21319 Cve: CVE-2024-0056 Cve: CVE-2024-0057 Cve: CVE-2024-20672 Url: https://github.com/dotnet/core/blob/main/release-notes/7.0/7.0.15/7.0.15.md Cert-bund: WID-SEC-2024-0040 Cert-bund: WID-SEC-2024-0039 Cert-bund: WID-SEC-2024-0037
Affected Nodes	192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 7.0.11`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 7.0.15 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple Vulnerabilities (Oct 2025)

Severity	▂▃▅▆▇
Description	This host is missing an important security update according to Microsoft security update October 2025. Affected systems: .NET Core runtime version 8.0.x prior to

	8.0.21, 9.0.x prior to 9.0.10 and .NET Core SDK version 8.0 prior to 8.0.121, 8.0.300 prior to 8.0.318, 8.0.400 prior to 8.0.415, 9.0.x prior to 9.0.111, and 9.0.300 prior to 9.0.306. Impact: Successful exploitation allows an attacker to elevate privileges, bypass security restrictions and disclose information.
CVSS3	9.9
Recommendation	Update .NET Core runtime to version 8.0.21 or 9.0.10 or later and update .NET Core SDK to version 8.0.121 or 8.0.318 or 8.0.415 or 9.0.111 or 9.0.306 or later.
References	Cve: CVE-2025-55248 Cve: CVE-2025-55315 Cve: CVE-2025-55247 Url: https://github.com/dotnet/core/blob/main/release-notes/9.0/9.0.10/9.0.10.md Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.21/8.0.21.md Cert-bund: WID-SEC-2025-2278
Affected Nodes	192.168.100.171 (ILAS3WKS88.infowerks.com) on port 0/tcp 192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 0/tcp 192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 0/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 8.0.10`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 8.0.21 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple Vulnerabilities - Windows

Severity	▂▃▅▆█
Description	.NET Core is prone to multiple vulnerabilities. Insight: Multiple flaws exist due to: - A security feature bypass vulnerability exists in ASP.NET where an unauthenticated user is able to bypass validation on Blazor server forms which could trigger unintended actions. - An elevation of privilege vulnerability exists in .NET where untrusted URIs provided to System.Net.WebRequest.Create can be used to inject arbitrary commands to backend FTP servers. Affected systems: .NET Core runtime 7.0 before 7.0.14, 6.0 before 6.0.25, 8.0 before 8.0.0 and .NET Core SDK before 7.0.114, 6.0.317, 8.0.100. Impact: Successful exploitation will allow an attacker to bypass security restrictions and elevate privileges on an affected system.
CVSS3	9.8
Recommendation	Upgrade .NET Core runtimes to versions 7.0.14 or 6.0.25 or 8.0.0 or later or upgrade .NET Core SDK to versions 6.0.317 or 7.0.114 or 8.0.100 or later.
References	Cve: CVE-2023-36049 Cve: CVE-2023-36558 Url: https://github.com/dotnet/announcements/issues/288 Url: https://github.com/dotnet/announcements/issues/287 Cert-bund: WID-SEC-2023-2895

Affected Nodes	192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 7.0.11`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 7.0.14 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

7zip Authentication Bypass Vulnerability - Windows

Severity	▮▮▮▮▯
Description	7zip is prone to an authentication bypass vulnerability. Insight: 7-Zip through 18.01 on Windows implements the Large memory pages option by calling the LsaAddAccountRights function to add the SeLockMemoryPrivilege privilege to the user's account, which makes it easier for attackers to bypass intended access restrictions by using this privilege in the context of a sandboxed process. Affected systems: 7zip through version 18.01.
CVSS3	8.8
Recommendation	Upgrade to 7zip version 18.03 or later.
References	Cve: CVE-2018-10172 Url: https://sourceforge.net/p/sevenzip/discussion/45797/thread/e730c709/?limit=25&page=1#b240
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 9.20`
	`Fixed version:     18.03`
	`Installation`
	`path / port:       Unable to find the install location`

7-Zip Mark-of-the-Web Bypass Vulnerability (Jan 2025) - Windows

Severity	▮▮▮▮▯
Description	7zip is prone to a mark-of-the-web bypass vulnerability. Insight: The flaw exists due to an incomplete implementation or design oversight in 7-Zip's handling of the Mark-of-the-Web mechanism when extracting files from archives. Affected systems: 7zip version prior to 24.09 on Windows. Impact: Successful exploitation allows an attacker to bypass the 'Mark-of-the-Web' security feature in Windows and execute arbitrary code in the context of the current user.
CVSS3	7.0
Recommendation	Update to version 24.09 or later.
References	Cve: CVE-2025-0411 Cisa: Known Exploited Vulnerability (KEV) catalog Url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog Url: https://www.zerodayinitiative.com/advisories/ZDI-25-045/ Url: https://www.trendmicro.com/en_us/research/25/a/cve-2025-0411-ukrainian-organizations-targeted.html Cert-bund: WID-SEC-2025-0129
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp 192.168.101.206 (ILAS4BCC2.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 24.08`
	`Fixed version:     24.09`

	`Installation`
	`path / port:       Unable to find the install location`

7-Zip Multiple Vulnerabilities (Jul 2025) - Windows

Severity	▂▃▅▆▇
Description	7zip is prone to multiple vulnerabilities. Affected systems: 7zip prior to version 25.0.0 on Windows. Impact: Successful exploitation allows an attacker to execute code in the context of a service account and conduct denial of service attacks.
CVSS3	7.5
Recommendation	Update to version 25.0.0 or later.
References	Cve: CVE-2025-53816 Cve: CVE-2025-53817 Cve: CVE-2025-11001 Cve: CVE-2025-11002 Url: https://securitylab.github.com/advisories/GHSL-2025-059_7-Zip/ Url: https://securitylab.github.com/advisories/GHSL-2025-058_7-Zip/ Url: https://www.zerodayinitiative.com/advisories/ZDI-25-949/ Url: https://www.zerodayinitiative.com/advisories/ZDI-25-950/ Cert-bund: WID-SEC-2025-2359 Cert-bund: WID-SEC-2025-2261 Cert-bund: WID-SEC-2025-1590
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp 192.168.101.206 (ILAS4BCC2.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 9.20`
	`Fixed version:     25.0.0`
	`Installation`
	`path / port:       Unable to find the install location`

7-Zip Qcow Handler Infinite Loop DoS Vulnerability - Windows

Severity	▂▃▅▆▇
Description	7zip is prone to a qcow handler infinite loop denial of service (DoS) vulnerability. Insight: The flaw exists due to an infinite loop in the CopyCoder processing streams. Affected systems: 7zip version prior to 24.08 on Windows. Impact: Successful exploitation allows an attacker to conduct denial of service attacks.
Recommendation	Update to version 24.08 or later.
References	Cve: CVE-2024-11612 Url: https://www.zerodayinitiative.com/advisories/ZDI-24-1606/ Cert-bund: WID-SEC-2025-0818 Cert-bund: WID-SEC-2024-3527
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 9.20`
	`Fixed version:     24.08`
	`Installation`
	`path / port:       Unable to find the install location`

7zip RAR Denial of Service Vulnerability - Windows

Severity	▂▃▅▆▇
Description	7zip is prone to a RAR Denial of Service Vulnerability. Insight: Incorrect initialization logic of RAR decoder objects in 7-Zip 18.03 and before can lead to usage of uninitialized memory, allowing remote attackers to cause a denial of service (segmentation fault) or execute arbitrary code via a crafted RAR archive. Affected systems: 7zip through version 18.03.
CVSS3	7.8
Recommendation	Upgrade to 7zip version 18.05 or later.
References	Cve: CVE-2018-10115 Url: https://sourceforge.net/p/sevenzip/discussion/45797/thread/e730c709/?limit=25&page=1#b240 Cert-bund: CB-K18/0647
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 9.20`
	`Fixed version:     18.05`
	`Installation`
	`path / port:       Unable to find the install location`

7Zip UDF CInArchive::ReadFileItem Code Execution Vulnerability

Severity	▂▃▅▆▇
Description	7Zip is prone to a code execution vulnerability. Insight: The flaw exists due to an out of bound read error in the 'CInArchive::ReadFileItem method' functionality. Affected systems: 7Zip version 9.20 and 15.05 beta. Impact: Successful exploitation will allow remote attackers to cause a denial of service or code execution.
CVSS3	8.8
Recommendation	Upgrade to 7Zip version 16.04 or later.
References	Cve: CVE-2016-2335 Url: http://www.talosintel.com/reports/TALOS-2016-0094/ Url: http://lists.opensuse.org/opensuse-updates/2016-06/msg00004.html Url: http://www.7-zip.org/history.txt Cert-bund: CB-K16/1620 Cert-bund: CB-K16/0877 Cert-bund: CB-K16/0744
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 9.20`
	`Fixed version:     16.04`

7-Zip Zstandard Decompression Integer Underflow Vulnerability - Windows

Severity	▂▃▅▆▇
Description	7zip is prone to a zstandard decompression integer underflow vulnerability. Insight: The flaw exists due to lack of input data

	validation in the Zstandard decompression feature in 7-Zip. Affected systems: 7zip version prior to 24.07 on Windows. Impact: Successful exploitation allows an attacker to perform remote code execution.
CVSS3	7.8
Recommendation	Update to version 24.07 or later.
References	Cve: CVE-2024-11477 Url: https://www.zerodayinitiative.com/advisories/ZDI-24-1532/ Cert-bund: WID-SEC-2024-3512
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 9.20`
	`Fixed version:     24.07`
	`Installation`
	`path / port:       Unable to find the install location`

Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-26) - Windows	
Severity	▮▮▮▮▯
Description	Adobe Flash Player within Microsoft Edge or Internet Explorer is prone to an use after free vulnerability. Insight: The flaw exists due to an use after free error. Affected systems: Adobe Flash Player prior to 32.0.0.192 within Microsoft Edge or Internet Explorer on, Windows 10 Version 1607 for x32/x64 Edition, Windows 10 Version 1703 for x32/x64 Edition, Windows 10 Version 1709 for x32/x64 Edition, Windows 10 Version 1803 for x32/x64 Edition, Windows 10 Version 1809 for x32/x64 Edition, Windows 10 x32/x64 Edition, Windows 8.1 for x32/x64 Edition, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 Impact: Successful exploitation allows attackers to conduct arbitrary code execution in the context of current user.
CVSS3	8.8
Recommendation	Upgrade to Adobe Flash Player 32.0.0.192 or later. Please see the references for more information.
References	Cve: CVE-2019-7837 Url: https://helpx.adobe.com/security/products/flash-player/apsb19-26.html Cert-bund: CB-K19/0418
Affected Nodes	192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp

Additional Output	`Vulnerable range:  Less than 32.0.0.192`
	`File checked:      C:\Windows\SysWOW64\Flashplayerapp.exe`
	`File version:      11.8.800.133`

Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-30) - Windows

Severity	▂▃▅▆▇
Description	Adobe Flash Player within Microsoft Edge or Internet Explorer is prone to an use after free vulnerability. Insight: The flaw exists due to an use after free error. Affected systems: Adobe Flash Player prior to 32.0.0.207 within Microsoft Edge or Internet Explorer on, Windows 10 Version 1607 for x32/x64 Edition, Windows 10 Version 1703 for x32/x64 Edition, Windows 10 Version 1709 for x32/x64 Edition, Windows 10 Version 1803 for x32/x64 Edition, Windows 10 Version 1809 for x32/x64 Edition, Windows 10 x32/x64 Edition, Windows 8.1 for x32/x64 Edition, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 Impact: Successful exploitation allows attackers to conduct arbitrary code execution in the context of current user.
CVSS3	8.8
Recommendation	Upgrade to Adobe Flash Player 32.0.0.207 or later. Please see the references for more information.
References	Cve: CVE-2019-7845 Url: https://helpx.adobe.com/security/products/flash-player/apsb19-30.html Cert-bund: CB-K19/0494
Affected Nodes	192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp

Additional Output	`Vulnerable range:  Less than 32.0.0.207`
	`File checked:      C:\Windows\SysWOW64\Flashplayerapp.exe`
	`File version:      11.8.800.133`

Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB20-06) - Windows

Severity	▂▃▅▆▇
Description	Adobe Flash Player is prone to an arbitrary code execution vulnerability. Insight: The flaw exists due to a type confusion issue. Affected systems: Adobe Flash Player prior to 32.0.0.330 within Microsoft Edge or Internet Explorer on, Windows 10 Version 1607 for x32/x64 Edition,

	Windows 10 Version 1709 for x32/x64 Edition, Windows 10 Version 1803 for x32/x64 Edition, Windows 10 Version 1809 for x32/x64 Edition, Windows 10 Version 1903 for x32/x64 Edition, Windows 10 Version 1909 for x32/x64 Edition, Windows 10 x32/x64 Edition, Windows 8.1 for x32/x64 Edition, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 Impact: Successful exploitation allows attackers to execute arbitrary code.
CVSS3	8.8
Recommendation	Update to Adobe Flash Player 32.0.0.330 or later.
References	Cve: CVE-2020-3757 Url: https://helpx.adobe.com/security/products/flash-player/apsb20-06.html Cert-bund: CB-K20/0121
Affected Nodes	192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp

Additional Output	`Vulnerable range:  Less than 32.0.0.330`
	`File checked:      C:\WINDOWS\SysWOW64\Flashplayerapp.exe`
	`File version:      32.0.0.255`

Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB20-58) - Windows	
Severity	▂▃▅▆█
Description	Adobe Flash Player is prone to an arbitrary code execution vulnerability. Insight: The flaw exists due to a null pointer dereference error. Affected systems: Adobe Flash Player prior to 32.0.0.445 within Microsoft Edge or Internet Explorer on: Windows 10 Version 1607 for x32/x64 Edition Windows 10 Version 1703 for x32/x64 Edition Windows 10 Version 1709 for x32/x64 Edition Windows 10 Version 1803 for x32/x64 Edition Windows 10 Version 1809 for x32/x64 Edition Windows 10 Version 1903 for x32/x64 Edition Windows 10 Version 1909 for x32/x64 Edition

	Windows 10 Version 2004 for x32/x64 Edition Windows 10 x32/x64 Edition Windows 8.1 for x32/x64 Edition Windows Server 2012/2012 R2 Windows Server 2016 Windows Server 2019 Impact: Successful exploitation allows attackers to execute arbitrary code.
CVSS3	8.8
Recommendation	Update to Adobe Flash Player 32.0.0.445 or later.
References	Cve: CVE-2020-9746 Url: https://helpx.adobe.com/security/products/flash-player/apsb20-58.html Cert-bund: CB-K20/0981
Affected Nodes	192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.184 (ilas3db140.infowerks.com) on port 0/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.101.185 (ilas3stor01.infowerks.com) on port 0/tcp

Additional Output	`Vulnerable range:  Less than 32.0.0.445`
	`File checked:      C:\Windows\SysWOW64\Flashplayerapp.exe`
	`File version:      32.0.0.330`

Apache Tomcat Clustering DoS Vulnerability (May 2022)

Severity	▮▮▮▮▯
Description	Apache Tomcat is prone to a denial of service (DoS) vulnerability when running with enabled Tomcat clustering over an untrusted network. Insight: The documentation for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks. Affected systems: - The documentation in Apache Tomcat 8.5.38 through 8.5.78, 9.0.13 through 9.0.62, 10.0.0-M1 through 10.0.20 and 10.1.0-M1 to 10.1.0-M14 - Apache Tomcat when running with enabled Tomcat clustering over an untrusted network
CVSS3	7.5
Recommendation	- Don't run Apache Tomcat with enabled Tomcat clustering over an untrusted network - Update Apache Tomcat to version 10.1.0-M15, 10.0.21, 9.0.63, 8.5.79 or later to receive the corrected / updated documentation
References	Cve: CVE-2022-29885 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.0-M15 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.21 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.63 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.79 Url: https://lists.apache.org/thread/548bnqoxvp0rqqq2yyj90l0xvwhq087d Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2022-1780

	Cert-bund: WID-SEC-2022-1767 Cert-bund: WID-SEC-2022-0799 Cert-bund: WID-SEC-2022-0467 Cert-bund: CB-K22/0597
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     See solution information`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat DoS Vulnerability (Feb 2023) - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to a denial of service (DoS) vulnerability. Insight: Apache Tomcat uses a packaged renamed copy of Apache Commons FileUpload to provide the file upload functionality defined in the Jakarta Servlet specification. Apache Tomcat was, therefore, also vulnerable to the Apache Commons FileUpload vulnerability CVE-2023-24998 as there was no limit to the number of request parts processed. This resulted in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads. Affected systems: Apache Tomcat versions through 8.5.84, 9.0.0-M1 through 9.0.70, 10.x through 10.1.4 and 11.0.0-M1 only.
CVSS3	7.5
Recommendation	Update to version 8.5.85, 9.0.71, 10.1.5, 11.0.0-M3 or later.
References	Cve: CVE-2023-24998 Url: https://lists.apache.org/thread/g16kv0xpp272htz107molwbbgdrqrdk1 Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.5 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.71 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.85 Url: https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrrdoy Cert-bund: WID-SEC-2025-0810 Cert-bund: WID-SEC-2024-1652 Cert-bund: WID-SEC-2024-1642 Cert-bund: WID-SEC-2024-1637 Cert-bund: WID-SEC-2024-1622 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-0890 Cert-bund: WID-SEC-2024-0888 Cert-bund: WID-SEC-2024-0794 Cert-bund: WID-SEC-2024-0124 Cert-bund: WID-SEC-2024-0117 Cert-bund: WID-SEC-2024-0054 Cert-bund: WID-SEC-2023-2688 Cert-bund: WID-SEC-2023-2675 Cert-bund: WID-SEC-2023-2674 Cert-bund: WID-SEC-2023-2625 Cert-bund: WID-SEC-2023-2309 Cert-bund: WID-SEC-2023-2031 Cert-bund: WID-SEC-2023-1817 Cert-bund: WID-SEC-2023-1815 Cert-bund: WID-SEC-2023-1813 Cert-bund: WID-SEC-2023-1812 Cert-bund: WID-SEC-2023-1811 Cert-bund: WID-SEC-2023-1809 Cert-bund: WID-SEC-2023-1808 Cert-bund: WID-SEC-2023-1807

	Cert-bund: WID-SEC-2023-1794 Cert-bund: WID-SEC-2023-1792 Cert-bund: WID-SEC-2023-1791 Cert-bund: WID-SEC-2023-1784 Cert-bund: WID-SEC-2023-1783 Cert-bund: WID-SEC-2023-1782 Cert-bund: WID-SEC-2023-1424 Cert-bund: WID-SEC-2023-1142 Cert-bund: WID-SEC-2023-1021 Cert-bund: WID-SEC-2023-1017 Cert-bund: WID-SEC-2023-1016 Cert-bund: WID-SEC-2023-1012 Cert-bund: WID-SEC-2023-1007 Cert-bund: WID-SEC-2023-1005 Cert-bund: WID-SEC-2023-0609 Cert-bund: WID-SEC-2023-0433
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     8.5.85`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat DoS Vulnerability (Jul 2024) - Windows

Severity	▮▮▮▮▯
Description	Apache Tomcat is prone to a denial of service (DoS) vulnerability. Insight: When processing an HTTP/2 stream, Tomcat did not handle some cases of excessive HTTP headers correctly. This led to a miscounting of active HTTP/2 streams which in turn led to the use of an incorrect infinite timeout which allowed connections to remain open which should have been closed. Affected systems: Apache Tomcat versions prior to 9.0.90, 10.x through 10.1.24 and 11.0.0-M1 through 11.0.0-M20. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by this flaw. If you disagree with this assessment and want to accept the risk please create an override for this result.
Recommendation	Update to version 9.0.90, 10.1.25, 11.0.0-M21 or later.
References	Cve: CVE-2024-34750 Url: https://lists.apache.org/thread/4kqf0bc9gxymjc2x7v3p7dvplnl77y8l Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M21 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.25 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.90 Cert-bund: WID-SEC-2025-0163 Cert-bund: WID-SEC-2025-0161 Cert-bund: WID-SEC-2025-0148 Cert-bund: WID-SEC-2025-0144 Cert-bund: WID-SEC-2025-0143 Cert-bund: WID-SEC-2024-3197 Cert-bund: WID-SEC-2024-3195 Cert-bund: WID-SEC-2024-2100 Cert-bund: WID-SEC-2024-1905 Cert-bund: WID-SEC-2024-1522
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.90`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat DoS Vulnerability (Jul 2025) - Windows

Severity	📶
Description	Apache Tomcat is prone to a denial of service (DoS) vulnerability. Insight: A race condition on connection close could trigger a JVM crash when using the APR/Native connector leading to a DoS. This was particularly noticeable with client initiated closes of HTTP/2 connections. Affected systems: Apache Tomcat version 9.0.106 and prior. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
Recommendation	Update to version 9.0.107 or later.
References	Cve: CVE-2025-52434 Url: https://lists.apache.org/thread/gxgh65004f25y8519coth6w7vchww030 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.107 Cert-bund: WID-SEC-2025-1905 Cert-bund: WID-SEC-2025-1468
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.107`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat DoS Vulnerability (Jun 2019) - Windows

Severity	📶
Description	Apache Tomcat is prone to a denial of service vulnerability in the HTTP/2 implementation. Insight: The HTTP/2 implementation accepts streams with excessive numbers of SETTINGS frames and also permitts clients to keep streams open without reading/writing request/response data. By keeping streams open for requests that utilises the Servlet API's blocking I/O, clients are able to cause server-side threads to block eventually leading to thread exhaustion and a DoS. Affected systems: Apache Tomcat 8.5.0 to 8.5.40 and 9.0.0.M1 to 9.0.19.
CVSS3	7.5
Recommendation	Update to version 8.5.41, 9.0.20 or later.
References	Cve: CVE-2019-10072 Url: http://tomcat.apache.org/security-9.html Url: http://tomcat.apache.org/security-8.html Cert-bund: WID-SEC-2024-0528 Cert-bund: CB-K20/1008 Cert-bund: CB-K20/0029 Cert-bund: CB-K19/0915 Cert-bund: CB-K19/0523
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.20`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat DoS Vulnerability (Jun 2020) - Windows

Severity	▁▂▃▅▇
Description	Apache Tomcat is prone to a denial of service vulnerability. Insight: A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive. Affected systems: Apache Tomcat 8.5.0 to 8.5.55, 9.0.0.M1 to 9.0.35 and 10.0.0-M1 to 10.0.0-M5.
CVSS3	7.5
Recommendation	Update to version 8.5.56, 9.0.36, 10.0.0-M6 or later.
References	Cve: CVE-2020-11996 Url: https://lists.apache.org/thread.html/r5541ef6b6b68b49f76fc4c45695940116da2bcbe0312ef204a00a2e0%40%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2022-1375 Cert-bund: CB-K20/1017 Cert-bund: CB-K20/0637 Cert-bund: CB-K20/0636
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.36`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat DoS Vulnerability (Mar 2019) - Windows

Severity	▁▂▃▅▇
Description	Apache Tomcat is prone to a denial of service vulnerability in the HTTP/2 implementation. Insight: The HTTP/2 implementation accepts streams with excessive numbers of SETTINGS frames and also permitts clients to keep streams open without reading/writing request/response data. By keeping streams open for requests that utilises the Servlet API's blocking I/O, clients are able to cause server-side threads to block eventually leading to thread exhaustion and a DoS. Affected systems: Apache Tomcat 8.5.0 to 8.5.37 and 9.0.0.M1 to 9.0.14.
CVSS3	7.5
Recommendation	Update to version 8.5.38, 9.0.16 or later.
References	Cve: CVE-2019-0199 Url: http://tomcat.apache.org/security-9.html Url: http://tomcat.apache.org/security-8.html Cert-bund: WID-SEC-2024-0528 Cert-bund: CB-K20/0543 Cert-bund: CB-K20/0029 Cert-bund: CB-K19/0235
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.16`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat DoS Vulnerability (Oct 2021) - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to a denial of service (DoS) vulnerability. Insight: The fix for bug 63362 introduced a memory leak. The object introduced to collect metrics for HTTP upgrade connections was not released for WebSocket connections once the WebSocket connection was closed. This created a memory leak that, over time, could lead to a denial of service via an OutOfMemoryError. Affected systems: Apache Tomcat 8.5.60 through 8.5.71, 9.0.40 through 9.0.53, 10.0.0-M10 through 10.0.11 and 10.1.0-M1 through 10.1.0-M5.
CVSS3	7.5
Recommendation	Update to version 8.5.72, 9.0.54, 10.0.12, 10.1.0-M6 or later.
References	Cve: CVE-2021-42340 Url: https://lists.apache.org/thread.html/r83a35be60f06aca2065f188ee542b9099695d57ced2e70e0885f905c%40%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2022-1909 Cert-bund: WID-SEC-2022-1908 Cert-bund: WID-SEC-2022-1375 Cert-bund: WID-SEC-2022-1121 Cert-bund: WID-SEC-2022-0757 Cert-bund: WID-SEC-2022-0749 Cert-bund: WID-SEC-2022-0740 Cert-bund: WID-SEC-2022-0624 Cert-bund: WID-SEC-2022-0607 Cert-bund: WID-SEC-2022-0577 Cert-bund: WID-SEC-2022-0169 Cert-bund: CB-K22/0468 Cert-bund: CB-K21/1078
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     8.5.72`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat DoS Vulnerability (Sep 2021) - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to a denial of service (DoS) vulnerability. Insight: When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service. Affected systems: Apache Tomcat 8.5.0 through 8.5.63, 9.0.0-M1 through 9.0.43 and 10.0.0-M1 through 10.0.2.
CVSS3	7.5

CVE	CVE-2021-41079
Recommendation	Update to version 8.5.64, 9.0.44, 10.0.4 or later.
References	Cve: CVE-2021-41079 Url: https://lists.apache.org/thread.html/rccdef0349fdf4fb73a4e4403095446d7fe6264e0a58e2df5c6799434%40%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-0673 Cert-bund: WID-SEC-2022-0615 Cert-bund: WID-SEC-2022-0607 Cert-bund: CB-K21/0983
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.44`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat 'Hostname Verification' Security Bypass Vulnerability - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to a security bypass vulnerability. Insight: The flaw exists due to a missing host name verification when using TLS with the WebSocket client. Affected systems: Apache Tomcat versions 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52 and 7.0.35 to 7.0.88 on Windows. Impact: Successful exploitation will allow an attacker to bypass certain security restrictions and perform unauthorized actions.
CVSS3	7.5
Recommendation	Upgrade to Apache Tomcat version 9.0.10 or 8.5.32 or 8.0.53 or 7.0.90 or later. Please see the references for more information.
References	Cve: CVE-2018-8034 Url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722091057.GA70283@minotaur.apache.org%3E Url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.10 Url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.53 Url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.32 Url: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.90 Cert-bund: WID-SEC-2024-1682 Cert-bund: WID-SEC-2024-0528 Cert-bund: CB-K19/0907 Cert-bund: CB-K19/0616 Cert-bund: CB-K19/0320 Cert-bund: CB-K18/1005 Cert-bund: CB-K18/0809
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.10`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat HTTP/2 Protocol DoS Vulnerability (MadeYouReset) - Windows

Severity	▂▃▅▆▇

Description	Apache Tomcat is prone to is prone to a denial of service (DoS) vulnerability in the HTTP/2 protocol dubbed 'MadeYouReset'. Insight: A mismatch caused by client-triggered server-sent stream resets between HTTP/2 specifications and the internal architectures of some HTTP/2 implementations may result in excessive server resource consumption leading to denial-of-service (DoS). By opening streams and then rapidly triggering the server to reset them, using malformed frames or flow control errors, an attacker can exploit incorrect stream accounting. Streams reset by the server are considered closed at the protocol level, even though backend processing continues. This allows a client to cause the server to handle an unbounded number of concurrent streams on a single connection. Affected systems: Apache Tomcat version 9.0.107 and prior, 10.x through 10.1.43 and 11.0.0-M1 through 11.0.9. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
Recommendation	Update to version 9.0.108, 10.1.44, 11.0.10 or later.
References	Cve: CVE-2025-8671 Cve: CVE-2025-48989 Url: https://lists.apache.org/thread/9ydfg0xr0tchmglcprhxgwhj0hfwxlyf Url: https://lists.apache.org/thread/p09775q0rd185m6zz98krg0fp45j8kr0 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.108 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.44 Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.10 Url: https://galbarnahum.com/posts/made-you-reset-intro Url: https://deepness-lab.org/publications/madeyoureset/ Url: https://kb.cert.org/vuls/id/767506 Url: https://thehackernews.com/2025/08/new-http2-madeyoureset-vulnerability.html Cert-bund: WID-SEC-2025-2373 Cert-bund: WID-SEC-2025-2361 Cert-bund: WID-SEC-2025-2360 Cert-bund: WID-SEC-2025-2357 Cert-bund: WID-SEC-2025-2356 Cert-bund: WID-SEC-2025-1830
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.108`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat HTTP/2 Vulnerability (Dec 2020) - Windows

Severity	▮▮▮▮▯
Description	Apache Tomcat is prone to an information disclosure vulnerability in HTTP/2. Insight: It was discovered that Apache Tomcat could re-use an HTTP request header value from the previous stream received on an HTTP/2 connection for the request associated with the subsequent stream. While this would most likely lead to an error and the closure of the HTTP/2 connection, it is possible that information could leak between requests. Affected systems: Apache Tomcat 8.5.0 to 8.5.59, 9.0.0.M1 to 9.0.39 and 10.0.0-M1 to 10.0.0-M9.
CVSS3	7.5
Recommendation	Update to version 8.5.60, 9.0.40, 10.0.0-M10 or later.
References	Cve: CVE-2020-17527 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.0-M10

	Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.40 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.60 Url: https://lists.apache.org/thread.html/rce5ac9a40173651d540babce59f6f3825f12c6d4e886ba00823b11e5%40%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2023-2466 Cert-bund: WID-SEC-2023-0065 Cert-bund: WID-SEC-2022-0624 Cert-bund: CB-K21/0421 Cert-bund: CB-K21/0418 Cert-bund: CB-K20/1195
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.40`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Information Disclosure Vulnerability (Mar 2021) - Windows

Severity	▁▂▃▄▅
Description	Apache Tomcat is prone to an information disclosure vulnerability. Insight: When responding to new h2c connection requests, Apache Tomcat could duplicate request headers and a limited amount of request body from one request to another meaning user A and user B could both see the results of user A's request. Affected systems: Apache Tomcat 8.5.x - 8.5.61, 9.0.0.M1 - 9.0.41 and 10.0.x prior to 10.0.1.
CVSS3	7.5
Recommendation	Update to version 8.5.63, 9.0.43, 10.0.2 or later.
References	Cve: CVE-2021-25122 Url: https://lists.apache.org/thread.html/r7b95bc248603360501f18c8eb03bb6001ec0ee3296205b34b07105b7@%3Cannounce.tomcat.apache.org%3E Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.2 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.43 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.63 Cert-bund: WID-SEC-2022-1375 Cert-bund: WID-SEC-2022-1099 Cert-bund: WID-SEC-2022-0624 Cert-bund: WID-SEC-2022-0607 Cert-bund: CB-K21/1094 Cert-bund: CB-K21/1081 Cert-bund: CB-K21/0770 Cert-bund: CB-K21/0222
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.43`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Local Privilege Escalation Vulnerability (Jan 2022) - Windows

Severity	▁▂▃▄▅
Description	Apache Tomcat is prone to a local privilege escalation vulnerability. Insight: The fix for bug CVE-2020-9484 introduced a time of check, time of use vulnerability that allowed a local attacker to perform actions with the privileges of the

	user that the Tomcat process is using. This issue is only exploitable when Tomcat is configured to persist sessions using the FileStore. Affected systems: Apache Tomcat 8.5.55 through 8.5.73, 9.0.35 through 9.0.56, 10.0.0-M5 through 10.0.14 and 10.1.0-M1 through 10.1.0-M8.
CVSS3	7.0
Recommendation	Update to version 8.5.75, 9.0.58, 10.0.16, 10.1.0-M10 or later. Note: This issue was fixed in Apache Tomcat 10.1.0-M9, 10.0.15, 9.0.57 and 8.5.74 but the release vote for those release candidates did not pass. Therefore, although users must download 10.1.0-M10, 10.0.16, 9.0.58 or 8.5.75 to obtain a version that includes a fix for this issue, versions 10.1.0-M9, 10.0.15, 9.0.57 and 8.5.74 are not included in the list of affected versions.
References	Cve: CVE-2022-23181 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.0-M10 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.16 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.58 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.75 Url: https://lists.apache.org/thread/0rzopt00r4dksgrtyxsmqjyhl8xrhv7p Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2023-1031 Cert-bund: WID-SEC-2022-1908 Cert-bund: WID-SEC-2022-1868 Cert-bund: WID-SEC-2022-1771 Cert-bund: WID-SEC-2022-1766 Cert-bund: WID-SEC-2022-1075 Cert-bund: WID-SEC-2022-0756 Cert-bund: WID-SEC-2022-0607 Cert-bund: WID-SEC-2022-0432 Cert-bund: WID-SEC-2022-0302 Cert-bund: WID-SEC-2022-0169 Cert-bund: CB-K22/0468 Cert-bund: CB-K22/0414 Cert-bund: CB-K22/0102
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     8.5.75`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat Multiple DoS Vulnerabilities (Jul 2020) - Windows

Severity	▮▮▮▮▯
Description	Apache Tomcat is prone to multiple denial of service vulnerabilities. Insight: The following vulnerabilitities exist: - HTTP/2 Denial of Service (CVE-2020-13934) - WebSocket Denial of Service (CVE-2020-13935) Affected systems: Apache Tomcat 8.5.1 to 8.5.56, 9.0.0.M5 to 9.0.36 and 10.0.0-M1 to 10.0.0-M6.
CVSS3	7.5
Recommendation	Update to version 8.5.57, 9.0.37, 10.0.0-M7 or later.
References	Cve: CVE-2020-13934 Cve: CVE-2020-13935 Url: https://lists.apache.org/thread.html/r61f411cf82488d6ec213063fc15feeeb88e31b0ca9c29652ee4f962e%40%3Cannounce.tomcat.apache.org%3E Url:

	https://lists.apache.org/thread.html/rd48c72bd3255bda87564d4da3791517c074d94f8a701f93b85752651%40%3Cannounce.tomcat.apache.org%3E Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.0-M7 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.37 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.57 Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2023-1048 Cert-bund: WID-SEC-2022-1375 Cert-bund: WID-SEC-2022-0519 Cert-bund: CB-K20/1030 Cert-bund: CB-K20/1021 Cert-bund: CB-K20/1017 Cert-bund: CB-K20/0717
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.37`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Multiple DoS Vulnerabilities (Jul 2025) - Windows	
Severity	▁▂▃▅▇
Description	Apache Tomcat is prone to multiple denial of service (DoS) vulnerabilities. Insight: The following flaws exist: - CVE-2025-52520: DoS due to overflow in file upload limit - CVE-2025-53506: DoS via excessive HTTP/2 streams Affected systems: Apache Tomcat version 9.0.106 and prior, 10.x through 10.1.42 and 11.0.0-M1 through 11.0.8. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
Recommendation	Update to version 9.0.107, 10.1.43, 11.0.9 or later.
References	Cve: CVE-2025-52520 Cve: CVE-2025-53506 Url: https://lists.apache.org/thread/trqq01bbxw6c92zx69kx2mw2qgmfy0o5 Url: https://lists.apache.org/thread/p09775q0rd185m6zz98krg0fp45j8kr0 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.107 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.43 Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.9 Cert-bund: WID-SEC-2025-1905 Cert-bund: WID-SEC-2025-1468
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.107`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat Multiple Vulnerabilities (Jun 2025) - Windows	
Severity	▁▂▃▅▇

Description	Apache Tomcat is prone to multiple vulnerabilities. Insight: The following flaws exist: - CVE-2025-48976: Denial of service (DoS) in Apache Commons FileUpload - CVE-2025-48988: DoS in multipart upload - CVE-2025-49125: Security constraint bypass for pre/post-resources Affected systems: Apache Tomcat version 9.0.105 and prior, 10.x through 10.1.41 and 11.0.0-M1 through 11.0.7. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
Recommendation	Update to version 9.0.106, 10.1.42, 11.0.8 or later.
References	Cve: CVE-2025-48976 Cve: CVE-2025-48988 Cve: CVE-2025-49125 Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.8 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.42 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.106 Url: https://lists.apache.org/thread/nzkqsok8t42qofgqfmck536mtyzygp18 Url: https://lists.apache.org/thread/m66cytbfrty9k7dc4cg6tl1czhsnbywk Url: https://www.openwall.com/lists/oss-security/2025/06/16/1 Url: https://www.openwall.com/lists/oss-security/2025/06/16/2 Url: https://github.com/Samb102/POC-CVE-2025-48988-CVE-2025-48976 Cert-bund: WID-SEC-2025-2373 Cert-bund: WID-SEC-2025-2372 Cert-bund: WID-SEC-2025-2371 Cert-bund: WID-SEC-2025-2369 Cert-bund: WID-SEC-2025-2366 Cert-bund: WID-SEC-2025-2362 Cert-bund: WID-SEC-2025-2361 Cert-bund: WID-SEC-2025-2360 Cert-bund: WID-SEC-2025-2359 Cert-bund: WID-SEC-2025-2357 Cert-bund: WID-SEC-2025-2356 Cert-bund: WID-SEC-2025-2355 Cert-bund: WID-SEC-2025-2353 Cert-bund: WID-SEC-2025-2351 Cert-bund: WID-SEC-2025-1562 Cert-bund: WID-SEC-2025-1560 Cert-bund: WID-SEC-2025-1559 Cert-bund: WID-SEC-2025-1335 Cert-bund: WID-SEC-2025-1334
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.106`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat Multiple Vulnerabilities (Oct 2023) - Windows

Severity	▮▮▮▮▯
Description	Apache Tomcat is prone to multiple vulnerabilities. Insight: The following flaws exist:

	- CVE-2023-42795: When recycling various internal objects, including the request and the response, prior to re-use by the next request/response, an error could cause Tomcat to skip some parts of the recycling process leading to information leaking from the current request/response to the next. - CVE-2023-44487: HTTP/2 rapid reset attack - CVE-2023-45648: A specially crafted, invalid trailer header could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy. Affected systems: Apache Tomcat versions 8.5.0 through 8.5.93, 9.0.0-M1 through 9.0.80, 10.0.0 through 10.1.13 and 11.0.0-M1 through 11.0.0-M11.
CVSS3	7.5
Recommendation	Update to version 8.5.94, 9.0.81, 10.1.14, 11.0.0-M12 or later.
References	Cve: CVE-2023-42795 Cve: CVE-2023-44487 Cve: CVE-2023-45648 Url: https://lists.apache.org/thread/065jfyo583490r9j2v73nhpyxdob56lw Url: https://lists.apache.org/thread/3m81kt8c2gtg4nkjfwt2hvt5l9ycx6vl Url: https://lists.apache.org/thread/2pv8yz1pyp088tsxfb7ogltk9msk0jdp Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M12 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.14 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.81 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.94 Url: https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack Url: https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/ Url: https://aws.amazon.com/blogs/security/how-aws-protects-customers-from-ddos-events/ Url: https://www.openwall.com/lists/oss-security/2023/10/10/6 Url: https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487 Url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog Cisa: Known Exploited Vulnerability (KEV) catalog Cert-bund: WID-SEC-2025-0225 Cert-bund: WID-SEC-2024-3684 Cert-bund: WID-SEC-2024-1652 Cert-bund: WID-SEC-2024-1643 Cert-bund: WID-SEC-2024-1642 Cert-bund: WID-SEC-2024-1307 Cert-bund: WID-SEC-2024-1248 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-1228 Cert-bund: WID-SEC-2024-0899 Cert-bund: WID-SEC-2024-0894 Cert-bund: WID-SEC-2024-0887 Cert-bund: WID-SEC-2024-0874 Cert-bund: WID-SEC-2024-0873 Cert-bund: WID-SEC-2024-0870 Cert-bund: WID-SEC-2024-0869 Cert-bund: WID-SEC-2024-0794 Cert-bund: WID-SEC-2024-0597 Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2024-0521 Cert-bund: WID-SEC-2024-0519 Cert-bund: WID-SEC-2024-0123 Cert-bund: WID-SEC-2024-0121 Cert-bund: WID-SEC-2024-0118 Cert-bund: WID-SEC-2024-0117 Cert-bund: WID-SEC-2024-0116 Cert-bund: WID-SEC-2024-0115 Cert-bund: WID-SEC-2024-0108 Cert-bund: WID-SEC-2024-0107 Cert-bund: WID-SEC-2024-0106 Cert-bund: WID-SEC-2024-0025

	Cert-bund: WID-SEC-2023-3146 Cert-bund: WID-SEC-2023-2993 Cert-bund: WID-SEC-2023-2963 Cert-bund: WID-SEC-2023-2788 Cert-bund: WID-SEC-2023-2723 Cert-bund: WID-SEC-2023-2655 Cert-bund: WID-SEC-2023-2628 Cert-bund: WID-SEC-2023-2627 Cert-bund: WID-SEC-2023-2618 Cert-bund: WID-SEC-2023-2611 Cert-bund: WID-SEC-2023-2606
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.81`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Privilege Escalation Vulnerability (Dec 2019) - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to a privilege escalation vulnerability. Insight: When Tomcat is configured with the JMX Remote Lifecycle Listener, a local attacker without access to the Tomcat process or configuration files is able to manipulate the RMI registry to perform a man-in-the-middle attack to capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and gain complete control over the Tomcat instance. Affected systems: Apache Tomcat 7.0.0 to 7.0.97, 8.5.0 to 8.5.47 and 9.0.0.M1 to 9.0.28.
CVSS3	7.0
Recommendation	Update to version 7.0.99, 8.5.49, 9.0.29 or later. As a mitigation disable Tomcat's JmxRemoteLifecycleListener and use the built-in remote JMX facilities provided by the JVM.
References	Cve: CVE-2019-12418 Url: https://lists.apache.org/thread.html/43530b91506e2e0c11cfbe691173f5df8c48f51b98262426d7493b67%40%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2023-1229 Cert-bund: CB-K20/0309 Cert-bund: CB-K19/1102
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.29`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat RCE Vulnerability (Apr 2019) - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to a remote code execution (RCE) vulnerability due to a bug in the way the JRE passes command line arguments to Windows. Insight: When running on Windows with enableCmdLineArguments enabled, the CGI Servlet is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disabled by default in Tomcat.

	Affected systems: Apache Tomcat 7.0.0 to 7.0.93, 8.5.0 to 8.5.39 and 9.0.0.M1 to 9.0.17.
CVSS3	8.1
Recommendation	Update to version 7.0.94, 8.5.40, 9.0.19 or later.
References	Cve: CVE-2019-0232 Url: http://tomcat.apache.org/security-9.html Url: http://tomcat.apache.org/security-8.html Url: http://tomcat.apache.org/security-7.html Cert-bund: WID-SEC-2024-0528 Cert-bund: CB-K20/0029 Cert-bund: CB-K19/0920 Cert-bund: CB-K19/0616 Cert-bund: CB-K19/0306
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.19`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat RCE Vulnerability (Mar 2021) - Windows	
Severity	▮▮▮▮▯
Description	Apache Tomcat is prone to a remote code execution (RCE) vulnerability due to an incomplete fix. Insight: The fix for CVE-2020-9484 was incomplete. When using a highly unlikely configuration edge case, the Tomcat instance is still vulnerable to CVE-2020-9484. Note that both the previously published prerequisites for CVE-2020-9484 also apply to this issue. Affected systems: Apache Tomcat 7.0.x - 7.0.107, 8.5.x - 8.5.61, 9.0.0.M1 - 9.0.41 and 10.0.x prior to 10.0.1.
CVSS3	7.0
Recommendation	Update to version 7.0.108, 8.5.63, 9.0.43, 10.0.2 or later.
References	Cve: CVE-2021-25329 Url: https://lists.apache.org/thread.html/rfe62fbf9d4c314f166fe8c668e50e5d9dd882a99447f26f0367474bf@%3Cannounce.tomcat.apache.org%3E Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.2 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.43 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.63 Url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.108 Cert-bund: WID-SEC-2022-1099 Cert-bund: WID-SEC-2022-0607 Cert-bund: CB-K21/0222
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.43`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat RCE Vulnerability (May 2020) - Windows	
Severity	▮▮▮▮▯
Description	Apache Tomcat is prone to a remote code execution (RCE) vulnerability.

	Insight: If: - an attacker is able to control the contents and name of a file on the server and - the server is configured to use the PersistenceManager with a FileStore and - the PersistenceManager is configured with sessionAttributeValueClassNameFilter Affected systems: Apache Tomcat 7.0.0 to 7.0.103, 8.5.0 to 8.5.54, 9.0.0.M1 to 9.0.34 and 10.0.0-M1 to 10.0.0-M4.
CVSS3	7.0
Recommendation	Update to version 7.0.104, 8.5.55, 9.0.35, 10.0.0-M5 or later.
References	Cve: CVE-2020-9484 Url: https://lists.apache.org/thread.html/r77eae567ed829da9012cadb29af17f2df8fa23bf66faf88229857bb1%40%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2022-1870 Cert-bund: WID-SEC-2022-0607 Cert-bund: WID-SEC-2022-0432 Cert-bund: WID-SEC-2022-0302 Cert-bund: CB-K21/1094 Cert-bund: CB-K21/0069 Cert-bund: CB-K20/1017 Cert-bund: CB-K20/0494
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.35`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Request Mix-up Vulnerability (May 2022) - Windows

Severity	▮▮▮▮▯
Description	Apache Tomcat is prone to a request mix-up vulnerability. Insight: If a web application sends a WebSocket message concurrently with the WebSocket connection closing, it is possible that the application will continue to use the socket after it has been closed. The error handling triggered in this case could cause the a pooled object to be placed in the pool twice. This could result in subsequent connections using the same object concurrently which could result in data being returned to the wrong use and/or other errors. Affected systems: Apache Tomcat 8.5.0 through 8.5.75 and 9.0.0.M1 through 9.0.20.
CVSS3	8.6
Recommendation	Update to version 8.5.76, 9.0.21 or later.
References	Cve: CVE-2022-25762 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.21 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.76 Url: https://lists.apache.org/thread/tkmozotlgcrpvhx5vt6kw0pxtfx11k67 Cert-bund: WID-SEC-2022-1335 Cert-bund: WID-SEC-2022-1228 Cert-bund: WID-SEC-2022-0899 Cert-bund: WID-SEC-2022-0740 Cert-bund: CB-K22/0600
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     8.5.76`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat Request Smuggling Vulnerability (Nov 2023) - Windows	
Severity	▂▃▅▆█
Description	Apache Tomcat is prone to a request smuggling vulnerability. Insight: Tomcat does not correctly parse HTTP trailer headers. A specially crafted trailer header that exceeds the header size limit could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy. Affected systems: Apache Tomcat versions 8.5.0 through 8.5.95, 9.0.0-M1 through 9.0.82, 10.1.0-M1 through 10.1.15 and 11.0.0-M1 through 11.0.0-M10.
CVSS3	7.5
Recommendation	Update to version 8.5.96, 9.0.83, 10.1.16, 11.0.0-M11 or later.
References	Cve: CVE-2023-46589 Url: https://lists.apache.org/thread/0rqq6ktozqc42ro8hhxdmmdjm1k1tpxr Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M11 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.16 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.83 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.96 Cert-bund: WID-SEC-2025-0810 Cert-bund: WID-SEC-2024-1653 Cert-bund: WID-SEC-2024-1652 Cert-bund: WID-SEC-2024-1642 Cert-bund: WID-SEC-2024-1248 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-0899 Cert-bund: WID-SEC-2024-0890 Cert-bund: WID-SEC-2024-0873 Cert-bund: WID-SEC-2024-0869 Cert-bund: WID-SEC-2024-0769 Cert-bund: WID-SEC-2024-0119 Cert-bund: WID-SEC-2024-0108 Cert-bund: WID-SEC-2024-0106 Cert-bund: WID-SEC-2024-0101 Cert-bund: WID-SEC-2024-0094 Cert-bund: WID-SEC-2023-3020
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     8.5.96`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat Request Smuggling Vulnerability (Oct 2022) - Windows	
Severity	▂▃▅▆█
Description	Apache Tomcat is prone to a request smuggling vulnerability. Insight: If Tomcat is configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (the default for 8.5.x only), Tomcat does not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat is located behind a reverse proxy that also fails to reject the request with the invalid

	header. Affected systems: Apache Tomcat version 8.5.0 through 8.5.82, 9.0.0-M1 through 9.0.67, 10.0.0-M1 through 10.0.26 and 10.1.0.
CVSS3	7.5
Recommendation	Update to version 8.5.83, 9.0.68, 10.0.27, 10.1.1 or later.
References	Cve: CVE-2022-42252 Url: https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2023-2993 Cert-bund: WID-SEC-2023-1030 Cert-bund: WID-SEC-2023-1021 Cert-bund: WID-SEC-2023-1017 Cert-bund: WID-SEC-2023-0809 Cert-bund: WID-SEC-2023-0561 Cert-bund: WID-SEC-2023-0138 Cert-bund: WID-SEC-2023-0137 Cert-bund: WID-SEC-2023-0133 Cert-bund: WID-SEC-2023-0126 Cert-bund: WID-SEC-2023-0122 Cert-bund: WID-SEC-2022-1918
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.68`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Session Fixation Vulnerability (Aug 2025) - Windows	
Severity	▁▂▃▅▇
Description	Apache Tomcat is prone to a session fixation vulnerability. Insight: If the rewrite valve was enabled for a web application, an attacker was able to craft a URL that, if a victim clicked on it, would cause the victim's interaction with that resource to occur in the context of the attacker's session. Affected systems: Apache Tomcat versions prior to 9.0.106, 10.1.0-M1 through 10.1.41 and 11.0.0-M1 through 11.0.7.
Recommendation	Update to version 9.0.106, 10.1.42, 11.0.8 or later.
References	Cve: CVE-2025-55668 Url: https://lists.apache.org/thread/v6bknr96rl7l1qxkl1c03v0qdvbbqs47 Cert-bund: WID-SEC-2025-1905 Cert-bund: WID-SEC-2025-1826
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.106`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat Session Fixation Vulnerability (Dec 2019) - Windows	
Severity	▁▂▃▅▇
Description	Apache Tomcat is prone to a session fixation vulnerability. Insight: When using FORM authentication there was a narrow window where an attacker

	could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability. Affected systems: Apache Tomcat 7.0.0 to 7.0.98, 8.5.0 to 8.5.49 and 9.0.0.M1 to 9.0.29.
CVSS3	7.5
Recommendation	Update to version 7.0.99, 8.5.50, 9.0.30 or later.
References	Cve: CVE-2019-17563 Url: https://lists.apache.org/thread.html/8b4c1db8300117b28a0f3f743c0b9e3f964687a690cdf9662a884bbd%40%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2023-1229 Cert-bund: WID-SEC-2023-1049 Cert-bund: CB-K21/0071 Cert-bund: CB-K20/1030 Cert-bund: CB-K20/0318 Cert-bund: CB-K20/0309 Cert-bund: CB-K19/1102
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.30`
	`Installation`
	`path / port:       1311/tcp`

CUPS 2.4.7 Buffer Overflow Vulnerability	
Severity	▂▃▅▆▇
Description	CUPS is prone to a heap-based buffer overflow vulnerability. Insight: Due to failure in validating the length provided by an attacker-crafted PPD PostScript document, CUPS and libppd are susceptible to a heap-based buffer overflow and possibly code execution. Affected systems: CUPS version 2.4.6 and prior.
CVSS3	7.0
Recommendation	Update to version 2.4.7 or later.
References	Cve: CVE-2023-4504 Url: https://github.com/OpenPrinting/cups/security/advisories/GHSA-pf5r-86w9-678h Url: https://github.com/OpenPrinting/cups/releases/tag/v2.4.7 Cert-bund: WID-SEC-2024-2154 Cert-bund: WID-SEC-2023-2917 Cert-bund: WID-SEC-2023-2402
Affected Nodes	192.168.101.200 on port 631/tcp

Additional Output	`Installed version: 2.1`
	`Fixed version:     2.4.7`

Dell DRAC / iDRAC Default Credentials (HTTP)	
Severity	▂▃▅▆▇
Description	The remote Dell Remote Access Controller (DRAC) / Integrated Remote Access Controller (iDRAC) is using known default credentials for the HTTP login. Impact: This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration without requiring authentication.
Recommendation	Change the password.

References	Url: https://www.dell.com/support/contents/en-us/videos/videoplayer/how-to-log-in-to-idrac9-with-the-default-password/6336297377112 Url: https://www.dell.com/support/kbdoc/en-us/000177787/how-to-change-the-default-login-password-of-the-idrac-9
Affected Nodes	192.168.101.208 (ilas2db07.infowerks.com) on port 443/tcp

Additional Output	`It was possible to login with username 'root' and password 'calvin'.`
	
	`Vulnerable URL: https://ilas2db07.infowerks.com/data/login`
	`Result:         HTTP 200/201 status code and matching response: authResult0/authResult`

Deprecated SSH-1 Protocol Detection

Severity	▂▃▄▅▆
Description	The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptographic flaws. Affected systems: Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5). 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.
CVSS	7.5
CVE	CVE-2001-0361 CVE-2001-0572 CVE-2001-1473
Recommendation	Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.
References	Cve: CVE-2001-0361 Cve: CVE-2001-0572 Cve: CVE-2001-1473 Url: http://www.kb.cert.org/vuls/id/684820 Url: http://www.securityfocus.com/bid/2344 Url: http://xforce.iss.net/xforce/xfdb/6603 Cert-bund: CB-K15/1534
Affected Nodes	192.168.100.39 (ILAS1QA03.infowerks.com) on port 22/tcp 192.168.101.114 on port 22/tcp 192.168.101.115 on port 22/tcp

Additional Output	`The service is providing / accepting the following deprecated versions of the SSH protocol which have known cryptographic flaws:`
	
	`1.33`
	`1.5`

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)

Severity	▂▃▄▅▆
Description	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. Insight: - CVE-2002-20001: 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. - CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that '(appropriately) short exponents' can be used when there are adequate

	subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together. - CVE-2024-41996: Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations. The client may cause asymmetric resource consumption. 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 and validate the order of the public key. Impact: This vulnerability 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, also known as a D(HE)ater attack. There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.
CVSS3	7.5
Recommendation	- 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.
References	Cve: CVE-2002-20001 Cve: CVE-2022-40735 Cve: CVE-2024-41996 Url: https://dheatattack.gitlab.io/ Url: https://dheatattack.gitlab.io/details/ Url: https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol Url: https://github.com/Balasys/dheater Url: https://github.com/c0r0n3r/dheater Cert-bund: WID-SEC-2024-3056 Cert-bund: WID-SEC-2023-1886 Cert-bund: WID-SEC-2023-1352 Cert-bund: WID-SEC-2022-2251 Cert-bund: WID-SEC-2022-2000 Cert-bund: CB-K22/0224 Cert-bund: CB-K21/1276
Affected Nodes	192.168.100.14 on port 22/tcp 192.168.101.1 on port 22/tcp 192.168.101.3 on port 22/tcp 192.168.101.6 on port 22/tcp 192.168.101.8 (ilas1nas01.infowerks.com) on port 22/tcp 192.168.101.13 on port 22/tcp 192.168.101.17 (ilas1sw01.infowerks.com) on port 22/tcp 192.168.101.26 (ilas1qa02.infowerks.com) on port 22/tcp 192.168.101.29 (db-details.infowerks.com) on port 22/tcp 192.168.101.36 (ilas1sql03.infowerks.com) on port 22/tcp 192.168.101.39 on port 22/tcp 192.168.101.50 on port 22/tcp 192.168.101.51 (ilas1drn01.infowerks.com) on port 22/tcp 192.168.101.53 (ilas1drn03.infowerks.com) on port 22/tcp 192.168.101.91 (archive.infowerks.com) on port 22/tcp 192.168.101.92 on port 22/tcp

	192.168.101.93 (ilas1db04.infowerks.com) on port 22/tcp 192.168.101.114 on port 22/tcp 192.168.101.115 on port 22/tcp 192.168.101.189 on port 22/tcp 192.168.101.200 on port 22/tcp 192.168.101.208 (ilas2db07.infowerks.com) on port 22/tcp 192.168.101.215 on port 22/tcp 192.168.101.216 on port 22/tcp 192.168.101.225 on port 22/tcp 192.168.101.250 on port 22/tcp 192.168.199.1 on port 22/tcp 192.168.199.5 on port 22/tcp 192.168.199.6 on port 22/tcp 192.168.199.22 on port 22/tcp 192.168.199.30 on port 22/tcp 192.168.199.31 on port 22/tcp 192.168.199.74 on port 22/tcp 192.168.199.78 on port 22/tcp 192.168.199.79 on port 22/tcp 192.168.199.95 on port 22/tcp 192.168.199.204 on port 22/tcp 192.168.101.92 on port 1022/tcp 192.168.101.93 (ilas1db04.infowerks.com) on port 1022/tcp

Additional Output	`The remote SSH server supports the following DHE KEX algorithm(s):`
	
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group14-sha256`
	`diffie-hellman-group16-sha512`
	`diffie-hellman-group18-sha512`
	`diffie-hellman-group-exchange-sha256`

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)	
Severity	▮▮▮▮▯
Description	The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability. Insight: - CVE-2002-20001: 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. - CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that '(appropriately) short exponents' can be used when there are adequate subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together. - CVE-2024-41996: Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations. The client may cause asymmetric resource consumption. 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 and validate

	the order of the public key. Impact: This vulnerability 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, also known as a D(HE)ater attack. There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.
CVSS3	7.5
Recommendation	- 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.
References	Url: https://dheatattack.gitlab.io/ Cve: CVE-2002-20001 Cve: CVE-2022-40735 Cve: CVE-2024-41996 Url: https://dheatattack.gitlab.io/details/ Url: https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol Url: https://github.com/Balasys/dheater Url: https://github.com/c0r0n3r/dheater Cert-bund: WID-SEC-2024-3056 Cert-bund: WID-SEC-2023-1886 Cert-bund: WID-SEC-2023-1352 Cert-bund: WID-SEC-2022-2251 Cert-bund: WID-SEC-2022-2000 Cert-bund: CB-K22/0224 Cert-bund: CB-K21/1276
Affected Nodes	192.168.100.21 (ilas2ftp01.infowerks.com) on port 3389/tcp 192.168.100.39 (ILAS1QA03.infowerks.com) on port 3389/tcp 192.168.100.54 (ILAS2WKS27.infowerks.com) on port 3389/tcp 192.168.100.159 (ILAS3WKS81.infowerks.com) on port 3389/tcp 192.168.100.160 (ILAS3WKS82.infowerks.com) on port 3389/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 3389/tcp 192.168.100.170 (ILAS3WKS87.infowerks.com) on port 3389/tcp 192.168.100.171 (ILAS3WKS88.infowerks.com) on port 3389/tcp 192.168.100.200 (ilas3db05.infowerks.com) on port 3389/tcp 192.168.101.12 on port 443/tcp 192.168.101.24 on port 443/tcp 192.168.101.36 (ilas1sql03.infowerks.com) on port 5432/tcp 192.168.101.50 on port 5432/tcp 192.168.101.66 (ilas1sql02.infowerks.com) on port 3389/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 3389/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 3389/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 3389/tcp 192.168.101.85 (ilas3wks04.infowerks.com) on port 3389/tcp 192.168.101.93 (ilas1db04.infowerks.com) on port 5432/tcp 192.168.101.111 (ilas1dc01.infowerks.com) on port 3389/tcp 192.168.101.112 (icage0dc02.infowerks.com) on port 3389/tcp 192.168.101.114 on port 443/tcp 192.168.101.115 on port 443/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 3389/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 3389/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 3389/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 3389/tcp 192.168.101.184 (ilas3db140.infowerks.com) on port 3389/tcp 192.168.101.185 (ilas3stor01.infowerks.com) on port 3389/tcp

	192.168.101.186 (ilas3db154.infowerks.com) on port 3389/tcp 192.168.101.187 (ilas2db10.infowerks.com) on port 3389/tcp 192.168.101.189 on port 5432/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 3389/tcp 192.168.101.192 (ILAS3DB160.infowerks.com) on port 3389/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 3389/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 3389/tcp 192.168.101.198 (ILAS2IMG16.infowerks.com) on port 3389/tcp 192.168.101.208 (ilas2db07.infowerks.com) on port 443/tcp 192.168.101.250 on port 25/tcp 192.168.101.250 on port 8090/tcp 192.168.199.30 on port 5432/tcp 192.168.199.78 on port 443/tcp 192.168.199.95 on port 5432/tcp 192.168.101.141 (ILAS1WKS09.infowerks.com) on port 7070/tcp 192.168.101.24 on port 3033/tcp

Additional Output

```
'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CCM
TLS_DHE_RSA_WITH_AES_128_CCM_8
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_RSA_WITH_AES_256_CCM_8
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
```

.NET Core Denial of Service And Information Disclosure Vulnerabilities - Windows

Severity	▂▃▅▆▇
Description	.NET Core is prone to a denial of service (DoS) and an information disclosure vulnerability. Insight: Multiple flaws are due to: - .NET (Core) server applications providing WebSocket endpoints could be tricked into endlessly looping while trying to read a single WebSocket frame. - A JWT token is logged if it cannot be parsed. Affected systems: .NET Core runtime 5.0 before 5.0.9, 3.1 before 3.1.18, and 2.1 before 2.1.29 and .NET Core SDK 5.0 before 5.0.206, 3.1 before 3.1.118, and 2.1 before 2.1.525. Impact: Successful exploitation will allow an attacker to disclose sensitive information and also cause a denial of service condition.
CVSS3	7.5
Recommendation	Upgrade .NET Core runtimes to versions 5.0.9 or 3.1.18 or 2.1.29 or later or upgrade .NET Core SDK to versions 5.0.206 or 5.0.303 or 3.1.118 or 3.1.412 or 2.1.525 or 2.1.817 or later.
References	Cve: CVE-2021-26423 Cve: CVE-2021-34532

	Url: https://github.com/dotnet/announcements/issues/195 Url: https://github.com/dotnet/announcements/issues/194 Cert-bund: CB-K21/0854
Affected Nodes	192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 2.1.26`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 2.1.29`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Denial of Service Vulnerability - Windows

Severity	▂▃▅▆▇
Description	.NET Core and is prone to a denial of service (DoS) vulnerability. Insight: The flaw exists due to stack overflow vulnerability in .NET. Affected systems: .NET Core runtime 6.0 before 6.0.9, 3.1 before 3.1.29 and .NET Core SDK before 6.0.109, 6.0.304, 6.0.401, 3.1 before 3.1.423. Impact: Successful exploitation will allow an attacker to conduct DOS attack.
CVSS3	7.8
Recommendation	Upgrade .NET Core runtimes to versions 6.0.9 or 3.1.29 or later or upgrade .NET Core SDK to versions 6.0.109 or 6.0.304 or 6.0.401 or 3.1.423 or later.
References	Cve: CVE-2022-38010 Url: https://github.com/dotnet/core/blob/main/release-notes/6.0/6.0.9/6.0.9.md Url: https://github.com/dotnet/core/blob/main/release-notes/3.1/3.1.29/3.1.29.md Cert-bund: WID-SEC-2022-1404
Affected Nodes	192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 3.1.6`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 3.1.29 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core DoS Vulnerability (Feb 2024) - Windows

Severity	▂▃▅▆▇
Description	.NET Core is prone to a denial of service (DoS) vulnerability. Insight: The flaw exists due to a vulnerability exists in ASP.NET applications using SignalR where a malicious client can result in a DoS. Affected systems: .NET Core runtime version 6.0 prior to 6.0.26, 7.0 prior to 7.0.15 and 8.0 prior to 8.0.1.

	Impact: Successful exploitation will allow an attacker to cause a DoS on an affected system.
CVSS3	7.5
Recommendation	- Update .NET Core runtime to version 7.0.15, 6.0.268.0.1 or later - Update .NET Core SDK to version 6.0.419, 7.0.116, 8.0.102 or later
References	Cve: CVE-2024-21386 Url: https://github.com/dotnet/announcements/issues/295 Cert-bund: WID-SEC-2024-0365
Affected Nodes	192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 6.0.16`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 6.0.27 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core DoS Vulnerability (May 2020)

Severity	▂▃▅▆▇
Description	ASP.NET Core is prone to a denail-of-service vulnerability. Insight: The flaw exists due to an error when .NET Core or .NET Framework improperly handles web requests. Affected systems: ASP.NET Core version 2.1 and 3.1 Impact: Successful exploitation will allow an attacker to conduct DoS attacks.
CVSS3	7.5
Recommendation	Update to ASP.NET Core to 2.1.18 or 3.1.4 or later.
References	Cve: CVE-2020-1108 Url: https://github.com/dotnet/core/blob/master/release-notes/3.1/3.1.4/3.1.4.md Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.18/2.1.18.md Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1108 Cert-bund: CB-K20/0456
Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.6`
	`Fixed version:     2.1.8`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Elevation of Privilege Vulnerability (Mar 2025)

Severity	▂▃▅▆▇
Description	This host is missing an important security update according to Microsoft security update March 2025. Insight: The flaw exists due to an elevation of privilege vulnerability in .NET Core. Affected systems: .NET Core runtime version 8.0.x prior to 8.0.14, 9.0.x prior to 9.0.3 and .NET Core SDK version 8.0.x prior to 8.0.407 and 9.0.x prior to 9.0.201.

	Impact: Successful exploitation allows an attacker to elevate privileges.
CVSS3	7.0
Recommendation	Update .NET Core runtime to version 8.0.14 or 9.0.3 or later and update .NET Core SDK to version 8.0.407 or 9.0.201 or later.
References	Cve: CVE-2025-24070 Url: https://github.com/dotnet/core/blob/main/release-notes/9.0/9.0.3/9.0.3.md Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.14/8.0.14.md Cert-bund: WID-SEC-2025-0539
Affected Nodes	192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 0/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 8.0.3`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 8.0.14 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple Denial of Service Vulnerabilities (KB5014326)

Severity	📶
Description	This host is missing an important security update according to Microsoft KB5014326. Insight: Multiple flaws are due to an insufficient validation of user-supplied input in .NET and Visual Studio. Affected systems: .NET Core versions 3.1 prior to 3.1.25. Impact: Successful exploitation will allow an attacker to cause a denial of service condition on affected systems.
CVSS3	7.5
Recommendation	Upgrade .NET Core to version 3.1.25 or later.
References	Cve: CVE-2022-29145 Cve: CVE-2022-29117 Cve: CVE-2022-23267 Url: https://github.com/dotnet/core/blob/main/release-notes/3.1/3.1.25/3.1.25.md Cert-bund: WID-SEC-2022-0539 Cert-bund: CB-K22/0588
Affected Nodes	192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 3.1.6`
	`Fixed version:     3.1.25`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple Denial of Service Vulnerabilities (KB5036452)

Severity	📶

Description	.NET Core is prone to multiple denial of service vulnerabilities. Insight: These vulnerabilities exist: - CVE-2024-21392: .NET Denial of Service Vulnerability - CVE-2024-26190: Microsoft QUIC Denial of Service Vulnerability Affected systems: .NET Core runtime version 7.0 prior to 7.0.17, 8.0 prior to 8.0.3 and .NET Core SDK 7.0 prior to 7.0.407, 8.0 prior to 8.0.202 Impact: Successful exploitation will allow an attacker to cause denial of service on an affected system.
CVSS3	7.5
Recommendation	- Update .NET Core runtime to version 7.0.17 or 8.0.3 and .NET Core SDK to 7.0.407 or 8.0.202 or later.
References	Cve: CVE-2024-21392 Cve: CVE-2024-26190 Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.3/8.0.3.md Url: https://github.com/dotnet/core/blob/main/release-notes/7.0/7.0.17/7.0.17.md Cert-bund: WID-SEC-2024-0619 Cert-bund: WID-SEC-2024-0611
Affected Nodes	192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 7.0.11`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 7.0.17 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple DoS Vulnerabilities-01 (May 2019)

Severity	▁▂▃▅▇
Description	ASP.NET Core is prone to multiple DoS vulnerabilities. Insight: Multiple flaws exist due to - An error when .NET Core improperly process RegEx strings. - Multiple errors when .NET Core improperly handle web requests. Affected systems: ASP.NET Core 1.0.x prior to version 1.0.16 and 1.1.x prior to version 1.1.13 Impact: Successful exploitation will allow an attacker to conduct DoS condition.
CVSS3	7.5
Recommendation	Upgrade to ASP.NET Core 1.0.16 or 1.1.13 or later. Please see the references for more information.
References	Cve: CVE-2019-0820 Cve: CVE-2019-0980 Cve: CVE-2019-0981 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0820 Url: http://www.securityfocus.com/bid/108207 Url: http://www.securityfocus.com/bid/108232 Url: http://www.securityfocus.com/bid/108245 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0980 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0981 Url: https://github.com/dotnet/core/blob/master/release-notes/1.0/1.0.16/1.0.16.md

	Url: https://github.com/dotnet/core/blob/master/release-notes/1.1/1.1.13/1.1.13.md Cert-bund: CB-K19/0419
Affected Nodes	192.168.101.186 (ilas3db154.infowerks.com) on port 0/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 1.1.10`
	`Fixed version:     1.1.13`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple DoS Vulnerabilities-02 (May 2019)

Severity	▂▃▅▆▇
Description	ASP.NET Core is prone to multiple DoS vulnerabilities. Insight: Multiple flaws exist due to: - An error when .NET Core improperly process RegEx strings. - Multiple errors when .NET Core improperly handle web requests. Affected systems: ASP.NET Core 2.1.x prior to version 2.1.11 and 2.2.x prior to version 2.2.5 Impact: Successful exploitation will allow an attacker to conduct DoS condition.
CVSS3	7.5
Recommendation	Upgrade to ASP.NET Core 2.1.11 or 2.2.5 or later. Please see the references for more information.
References	Cve: CVE-2019-0820 Cve: CVE-2019-0980 Cve: CVE-2019-0981 Cve: CVE-2019-0982 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0820 Url: http://www.securityfocus.com/bid/108207 Url: http://www.securityfocus.com/bid/108232 Url: http://www.securityfocus.com/bid/108245 Url: http://www.securityfocus.com/bid/108208 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0980 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0981 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0982 Url: https://github.com/dotnet/core/blob/master/release-notes/2.2/2.2.5/2.2.5.md Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.11/2.1.11.md Cert-bund: CB-K19/0419
Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.6`
	`Fixed version:     2.1.11`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple DoS Vulnerabilities - Windows

Severity	▂▃▅▆▇
Description	.NET Core is prone to multiple denial of service vulnerabilities. Insight: Multiple flaws exist due to, - A vulnerability exists in the ASP.NET Core Kestrel web server where a

	malicious client may flood the server with specially crafted HTTP/2 requests, causing denial of service. - A null pointer vulnerability exists in MsQuic.dll which may lead to Denial of Service. - A memory leak vulnerability exists in MsQuic.dll which may lead to Denial of Service. Affected systems: .NET Core runtime 7.0 before 7.0.12 and .NET Core SDK before 7.0.402. Impact: Successful exploitation would allow an attacker to cause denial of service on an affected system.
CVSS3	7.5
Recommendation	Upgrade runtime to version 7.0.12 or SDK to 7.0.402 or later.
References	Cve: CVE-2023-38171 Cve: CVE-2023-36435 Cve: CVE-2023-44487 Url: https://github.com/dotnet/core/blob/main/release-notes/7.0/7.0.12/7.0.12.md Url: https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack Url: https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/ Url: https://aws.amazon.com/blogs/security/how-aws-protects-customers-from-ddos-events/ Url: https://www.openwall.com/lists/oss-security/2023/10/10/6 Url: https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487 Url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog Cisa: Known Exploited Vulnerability (KEV) catalog Cert-bund: WID-SEC-2025-0225 Cert-bund: WID-SEC-2024-3684 Cert-bund: WID-SEC-2024-1652 Cert-bund: WID-SEC-2024-1643 Cert-bund: WID-SEC-2024-1642 Cert-bund: WID-SEC-2024-1307 Cert-bund: WID-SEC-2024-1248 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-1228 Cert-bund: WID-SEC-2024-0899 Cert-bund: WID-SEC-2024-0894 Cert-bund: WID-SEC-2024-0887 Cert-bund: WID-SEC-2024-0874 Cert-bund: WID-SEC-2024-0873 Cert-bund: WID-SEC-2024-0870 Cert-bund: WID-SEC-2024-0869 Cert-bund: WID-SEC-2024-0794 Cert-bund: WID-SEC-2024-0597 Cert-bund: WID-SEC-2024-0521 Cert-bund: WID-SEC-2024-0519 Cert-bund: WID-SEC-2024-0123 Cert-bund: WID-SEC-2024-0121 Cert-bund: WID-SEC-2024-0118 Cert-bund: WID-SEC-2024-0117 Cert-bund: WID-SEC-2024-0116 Cert-bund: WID-SEC-2024-0115 Cert-bund: WID-SEC-2024-0108 Cert-bund: WID-SEC-2024-0107 Cert-bund: WID-SEC-2024-0106 Cert-bund: WID-SEC-2024-0025 Cert-bund: WID-SEC-2023-3146 Cert-bund: WID-SEC-2023-2993 Cert-bund: WID-SEC-2023-2788 Cert-bund: WID-SEC-2023-2723 Cert-bund: WID-SEC-2023-2655 Cert-bund: WID-SEC-2023-2628

	Cert-bund: WID-SEC-2023-2627 Cert-bund: WID-SEC-2023-2618 Cert-bund: WID-SEC-2023-2611 Cert-bund: WID-SEC-2023-2606
Affected Nodes	192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 7.0.11`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 7.0.12 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple Vulnerabilities (KB5041081)

Severity	▂▃▅▆█
Description	This host is missing an important security update according to Microsoft KB5041081. Insight: These vulnerabilities exist: - CVE-2024-38081: Elevation of Privilege Vulnerability - CVE-2024-38095: Denial of Service Vulnerability - CVE-2024-35264: Remote Code Execution Vulnerability - CVE-2024-30105: Denial of Service Vulnerability Affected systems: .NET Core runtime prior to version 8.0.7 and .NET Core SDK prior to version 8.0.303. Impact: Successful exploitation will allow an attacker to gain elevated privileges, conduct code execution and denial of service attacks.
CVSS3	8.1
Recommendation	Update .NET Core runtime to version 8.0.7 or later and update .NET Core SDK to version 8.0.303 later.
References	Cve: CVE-2024-38081 Cve: CVE-2024-38095 Cve: CVE-2024-35264 Cve: CVE-2024-30105 Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.7/8.0.7.md Cert-bund: WID-SEC-2024-1560
Affected Nodes	192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 8.0.3`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 8.0.7 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple Vulnerabilities (KB5042132)

Severity	▂▃▅▆█
Description	This host is missing an important security update according to Microsoft KB5042132. Insight: These vulnerabilities exist: - CVE-2024-38168: A vulnerability exists in .NET when an attacker through unauthenticated requests may trigger a Denial of Service in ASP.NET HTTP.sys web server.

	- CVE-2024-38167: A vulnerability exists in .NET runtime TlsStream which may result in Information Disclosure. Affected systems: .NET Core runtime prior to version 8.0.8 and .NET Core SDK prior to version 8.0.304. Impact: Successful exploitation will allow an attacker to disclose sensitive information and conduct denial of service attacks.
CVSS3	7.5
Recommendation	Update .NET Core runtime to version 8.0.8 or later and update .NET Core SDK to version 8.0.304 later.
References	Cve: CVE-2024-38168 Cve: CVE-2024-38167 Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.8/8.0.8.md Cert-bund: WID-SEC-2024-1821
Affected Nodes	192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp

Additional Output

```
Installed version: ASP .NET Core With Microsoft .NET Core runtimes 8.0.3
Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 8.0.8 or later
Installation
path / port:       Could not find the install location from registry
```

.NET Core Multiple Vulnerabilities (KB5045993)

Severity	▮▮▮▮▯
Description	This host is missing an important security update according to Microsoft KB5045993. Insight: These vulnerabilities exist: - CVE-2024-38229: Remote Code Execution Vulnerability - CVE-2024-43483: Denial of Service Vulnerability - CVE-2024-43484: Denial of Service Vulnerability - CVE-2024-43485: Denial of Service Vulnerability Affected systems: .NET Core runtime version 8.0.x prior to 8.0.10 and .NET Core SDK version 8.0.x prior to 8.0.403. Impact: Successful exploitation will allow an attacker to conduct code execution and denial of service attacks.
CVSS3	8.1
Recommendation	Update .NET Core runtime to version 8.0.10 or later and update .NET Core SDK to version 8.0.403 or later.
References	Cve: CVE-2024-38229 Cve: CVE-2024-43483 Cve: CVE-2024-43484 Cve: CVE-2024-43485 Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.10/8.0.10.md Cert-bund: WID-SEC-2024-3124
Affected Nodes	192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp

Additional Output

```
Installed version: ASP .NET Core With Microsoft .NET Core runtimes 8.0.3
Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 8.0.10 or later
```

	Installation path / port: Could not find the install location from registry

.NET Core Multiple Vulnerabilities (Sep 2019)

Severity	▮▮▮▮▯
Description	ASP.NET Core is prone to multiple vulnerabilities. Insight: Multiple flaws exist due to: - An error when .NET Core improperly handles web requests. - An error when a ASP.NET Core web application, created using vulnerable project templates fails to properly sanitize web requests. Affected systems: ASP.NET Core 2.1.x prior to version 2.1.13 and 2.2.x prior to version 2.2.7 Impact: Successful exploitation will allow an attacker to cause a denial of service condition and perform content injection attacks and run script in the security context of the logged-on user.
CVSS3	8.8
Recommendation	Upgrade to ASP.NET Core SDK 2.1.13 or 2.2.7 or later.
References	Cve: CVE-2019-1302 Cve: CVE-2019-1301 Url: https://github.com/dotnet/core/blob/master/release-notes/2.2/2.2.7/2.2.7.md Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.13/2.1.13.md Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1302 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1301 Cert-bund: CB-K19/0802
Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp
Additional Output	Installed version: 2.1.6 Fixed version: 2.1.13 Installation path / port: Could not find the install location from registry

.NET Core OData Denial of Service Vulnerability - Windows

Severity	▮▮▮▮▯
Description	.NET Core is prone to a denial of service vulnerability. Insight: The flaw exists when OData Library improperly handles web request Affected systems: .NET Core runtime 2.1 before 2.1.13, 2.2 before 2.2.7 and .NET Core SDK before 2.1.509, 2.1.606, 2.1.802, 2.2.109, 2.2.206 and 2.2.402. Impact: Successful exploitation would allow attackers to cause a denial of service against an OData web application.
CVSS3	7.5
Recommendation	Upgrade .NET Core runtimes to versions 2.1.13 or 2.2.7 or later or upgrade .NET Core SDK to versions 2.1.509 or 2.1.606 or 2.1.802 or 2.2.109 or 2.2.206 or 2.2.402 or later.
References	Cve: CVE-2018-8269 Url: https://github.com/aspnet/Announcements/issues/385

Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp
Additional Output	Installed version: ASP .NET Core With Microsoft .NET Core runtimes 2.1.6 Fixed version: ASP .NET Core With Microsoft .NET Core runtimes version 2.1.13 Installation path / port: Could not find the install location from registry

.NET Core Privilege Escalation Vulnerability (KB5037337)

Severity	▮▮▮▮▯
Description	This host is missing an important security update according to Microsoft KB5037337. Insight: The flaw exists due to an use-after-free vulnerability existing in WPF. Affected systems: .NET Core runtime prior to version 7.0.18 and .NET Core SDK prior to version 7.0.408. Impact: Successful exploitation allows an attacker to gain elevated privileges.
CVSS3	7.3
Recommendation	Update .NET Core runtime to version 7.0.18 or later and update .NET Core SDK to version 7.0.408 later.
References	Cve: CVE-2024-21409 Url: https://github.com/dotnet/core/blob/main/release-notes/7.0/7.0.18/7.0.18.md Cert-bund: WID-SEC-2024-0839
Affected Nodes	192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp
Additional Output	Installed version: ASP .NET Core With Microsoft .NET Core runtimes 7.0.11 Fixed version: ASP .NET Core With Microsoft .NET Core runtimes version 7.0.18 or later Installation path / port: Could not find the install location from registry

.NET Core Privilege Escalation Vulnerability (KB5037338)

Severity	▮▮▮▮▯
Description	This host is missing an important security update according to Microsoft KB5037338. Insight: The flaw exists due to an use-after-free vulnerability existing in WPF. Affected systems: .NET Core runtime prior to version 8.0.4 and .NET Core SDK prior to version 8.0.204. Impact: Successful exploitation allows an attacker to gain elevated privileges.
CVSS3	7.3
Recommendation	Update .NET Core runtime to version 8.0.4 or later and update .NET Core SDK to version 8.0.204 later.
References	Cve: CVE-2024-21409 Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.4/8.0.4.md Cert-bund: WID-SEC-2024-0839
Affected Nodes	192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 8.0.3`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 8.0.4 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core RCE Vulnerability (Jan 2025)	
Severity	▮▮▮▮▯
Description	This host is missing an important security update according to Microsoft security update January 2025. Insight: The flaw exists due to a remote code execution vulnerability in .NET Core. Affected systems: .NET Core runtime version 5.0.x prior to 5.0.4, 3.1.x prior to 3.1.13, 2.1.x prior to 2.1.26 and .NET Core SDK version 5.0.x prior to 5.0.104, 3.1.x prior to 3.1.113 and 2.1.x prior to 2.1.522. Impact: Successful exploitation allows an attacker to conduct remote code execution.
CVSS3	8.1
Recommendation	Update .NET Core runtime to version 5.0.4 or 3.1.13 or 2.1.26 or later and update .NET Core SDK to version 5.0.104 or 3.1.113 or 2.1.522 or later.
References	Cve: CVE-2021-26701 Url: https://github.com/dotnet/announcements/issues/178 Cert-bund: CB-K21/0158
Affected Nodes	192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 2.1.6`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 2.1.26 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core RCE Vulnerability (January-1 2025)	
Severity	▮▮▮▮▯
Description	This host is missing an important security update according to Microsoft security update January 2025. Insight: The flaw exists due to a remote code execution vulnerability in .NET Core. Affected systems: .NET Core runtime version 5.0.x prior to 5.0.3, 3.1.x prior to 3.1.12, 2.1.x prior to 2.1.25 and .NET Core SDK version 5.0.x prior to 5.0.103, 3.1.x prior to 3.1.112 and 2.1.x prior to 2.1.521. Impact: Successful exploitation allows an attacker to conduct remote code execution.
CVSS3	8.1
Recommendation	Update .NET Core runtime to version 5.0.3 or 3.1.12 or 2.1.25 or later and update .NET Core SDK to version 5.0.103 or 3.1.112 or 2.1.521 or later.

References	Cve: CVE-2021-24112 Url: https://github.com/dotnet/announcements/issues/176 Cert-bund: WID-SEC-2024-1656 Cert-bund: WID-SEC-2023-1805 Cert-bund: CB-K21/0158
Affected Nodes	192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 3.1.6`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 3.1.12 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core RCE Vulnerability (Jun 2025)

Severity	▂▃▅▆▇
Description	This host is missing an important security update according to Microsoft security update June 2025. Affected systems: .NET Core runtime version 8.0.x prior to 8.0.17, 9.0.x prior to 9.0.6 and .NET Core SDK version 8.0 prior to 8.0.117, 8.0.300 prior to 8.0.314, 8.0.400 prior to 8.0.411, 9.0.x prior to 9.0.107, 9.0.200 prior to 9.0.205 and 9.0.300 prior to 9.0.301. Impact: Successful exploitation allows an attacker to perform remote code execution.
CVSS3	7.5
Recommendation	Update .NET Core runtime to version 8.0.17 or 9.0.6 or later and update .NET Core SDK to version 8.0.117 or 8.0.314 or 8.0.411 or 9.0.107 or 9.0.205 or 9.0.301 or later.
References	Cve: CVE-2025-30399 Url: https://github.com/dotnet/core/blob/main/release-notes/9.0/9.0.6/9.0.6.md Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.17/8.0.17.md Cert-bund: WID-SEC-2025-1274
Affected Nodes	192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 0/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 8.0.11`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 8.0.17 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Remote Code Execution Vulnerability - Windows

Severity	▂▃▅▆▇
Description	.NET Core is prone to a remote code execution (RCE) vulnerability. Insight: The flaw is due to incorrect processing of user-supplied data in .NET. Affected systems: .NET Core runtime 7.0 before 7.0.1, 6.0 before 6.0.12, 3.1 before 3.1.32 and .NET Core SDK before 6.0.112 and 6.0.307,

	3.1 before 3.1.426 and 7.0 before 7.0.101. Impact: Successful exploitation will allow an attacker to disclose sensitive information and allow to spoof page content.
CVSS3	7.8
Recommendation	Upgrade .NET Core runtimes to versions 7.0.1 or 6.0.12 or 3.1.32 or later or upgrade .NET Core SDK to versions 6.0.112 or 6.0.307 or 7.0.101 or 3.1.426 or later.
References	Cve: CVE-2022-41089 Url: https://github.com/dotnet/core/blob/main/release-notes/3.1/3.1.32/3.1.32.md Url: https://github.com/dotnet/core/blob/main/release-notes/6.0/6.0.12/6.0.12.md Url: https://github.com/dotnet/core/blob/main/release-notes/7.0/7.0.1/7.0.1.md Cert-bund: WID-SEC-2022-2307
Affected Nodes	192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 3.1.13`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 3.1.32 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core SDK DoS Vulnerability (May 2020)

Severity	▂▃▅▆▇
Description	ASP.NET Core SDK is prone to a denail-of-service vulnerability. Insight: The flaw exists due to an error when .NET Core or .NET Framework improperly handles web requests. Affected systems: ASP.NET Core SDK 2.1.x prior to 2.1.514 and 3.1.x prior to 3.1.104 Impact: Successful exploitation will allow an attacker to conduct DoS attacks.
CVSS3	7.5
Recommendation	Update to ASP.NET Core SDK to 3.1.104 or 2.1.514 or later.
References	Cve: CVE-2020-1108 Url: https://github.com/dotnet/core/blob/master/release-notes/3.1/3.1.4/3.1.4.md Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.18/2.1.18.md Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1108 Cert-bund: CB-K20/0456
Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.500`
	`Fixed version:     2.1.514`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core SDK Multiple DoS Vulnerabilities-01 (May 2019)

Severity	▂▃▅▆▇
Description	ASP.NET Core SDK is prone to multiple DoS vulnerabilities. Insight: Multiple flaws exist due to

	- An error when .NET Core improperly process RegEx strings. - Multiple errors when .NET Core improperly handle web requests. Affected systems: ASP.NET Core SDK 1.x prior to version 1.1.13 Impact: Successful exploitation will allow an attacker to conduct DoS condition.
CVSS3	7.5
Recommendation	Upgrade to ASP.NET Core 1.1.13 (.NET Core SDK 1.1.13 includes .NET Core 1.0.16 Runtime) or 1.1.14 (.NET Core SDK 1.1.14 includes .NET Core 1.1.13 Runtime) or later. Please see the references for more information.
References	Cve: CVE-2019-0820 Cve: CVE-2019-0980 Cve: CVE-2019-0981 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0820 Url: http://www.securityfocus.com/bid/108207 Url: http://www.securityfocus.com/bid/108232 Url: http://www.securityfocus.com/bid/108245 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0980 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0981 Url: https://github.com/dotnet/core/blob/master/release-notes/1.0/1.0.16/1.0.16.md Url: https://github.com/dotnet/core/blob/master/release-notes/1.1/1.1.13/1.1.13.md Cert-bund: CB-K19/0419
Affected Nodes	192.168.101.186 (ilas3db154.infowerks.com) on port 0/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 1.1.11`
	`Fixed version:     1.1.13 or 1.1.14`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core SDK Multiple DoS Vulnerabilities-02 (May 2019)

Severity	▂▃▅▆▇
Description	ASP.NET Core SDK is prone to multiple DoS vulnerabilities. Insight: Multiple flaws exist due to: - An error when .NET Core improperly process RegEx strings. - Multiple errors when .NET Core improperly handle web requests. Affected systems: ASP.NET Core SDK 2.1.x prior to version 2.1.507 and 2.2.x prior to version 2.2.107 Impact: Successful exploitation will allow an attacker to conduct DoS condition.
CVSS3	7.5
Recommendation	Upgrade to ASP.NET Core SDK 2.1.507 or 2.2.107 or later.
References	Cve: CVE-2019-0820 Cve: CVE-2019-0980 Cve: CVE-2019-0981 Cve: CVE-2019-0982 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0820 Url: http://www.securityfocus.com/bid/108207 Url: http://www.securityfocus.com/bid/108232 Url: http://www.securityfocus.com/bid/108245

	Url: http://www.securityfocus.com/bid/108208 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0980 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0981 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0982 Url: https://github.com/dotnet/core/blob/master/release-notes/2.2/2.2.5/2.2.5.md Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.11/2.1.11.md Cert-bund: CB-K19/0419
Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.500`
	`Fixed version:     2.1.507`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core SDK Multiple Vulnerabilities (Sep 2019)

Severity	▂▃▅▆▇
Description	ASP.NET Core SDK is prone to multiple vulnerabilities. Insight: Multiple flaws exist due to: - An error when .NET Core improperly handles web requests. - An error when a ASP.NET Core web application, created using vulnerable project templates fails to properly sanitize web requests. Affected systems: ASP.NET Core SDK 2.1.x prior to version 2.1.509 and 2.2.x prior to version 2.2.109 Impact: Successful exploitation will allow an attacker to cause a denial of service condition and perform content injection attacks and run script in the security context of the logged-on user.
CVSS3	8.8
Recommendation	Upgrade to ASP.NET Core SDK 2.1.509 or 2.2.109 or later.
References	Cve: CVE-2019-1302 Cve: CVE-2019-1301 Url: https://github.com/dotnet/core/blob/master/release-notes/2.2/2.2.7/2.2.7.md Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.13/2.1.13.md Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1302 Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1301 Cert-bund: CB-K19/0802
Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.500`
	`Fixed version:     2.1.509`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core SDK Security Feature Bypass Vulnerability (Sep 2020)

Severity	▂▃▅▆▇
Description	ASP.NET Core SDK is prone to a security feature bypass vulnerability. Insight: The flaw exists due to an error in the way Microsoft ASP.NET Core parses encoded cookie names. Affected systems: ASP.NET Core SDK 2.1.x prior to 2.1.518 and 3.1.x prior to 3.1.108

	Impact: Successful exploitation will allow an attacker to bypass security restrictions.
CVSS3	7.5
Recommendation	The vendor has released updates. Please see the references for more information.
References	Cve: CVE-2020-1045 Url: https://github.com/dotnet/core/blob/master/release-notes/3.1/3.1.8/3.1.8.md Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.22/2.1.22.md Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1045 Cert-bund: CB-K20/0881
Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.500`
	`Fixed version:     2.1.518`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Security Feature Bypass Vulnerability (Sep 2020)

Severity	▮▮▮▮▯
Description	ASP.NET Core is prone to a security feature bypass vulnerability. Insight: The flaw exists due to an error in the way Microsoft ASP.NET Core parses encoded cookie names. Affected systems: ASP.NET Core version 2.1 and 3.1 Impact: Successful exploitation will allow an attacker to bypass security restrictions.
CVSS3	7.5
Recommendation	The vendor has released updates. Please see the references for more information.
References	Cve: CVE-2020-1045 Url: https://github.com/dotnet/core/blob/master/release-notes/3.1/3.1.8/3.1.8.md Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.22/2.1.22.md Url: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2020-1045 Cert-bund: CB-K20/0881
Affected Nodes	192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.20`
	`Fixed version:     2.1.22`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Spoofing Vulnerability (May 2025)

Severity	▮▮▮▮▯
Description	This host is missing an important security update according to Microsoft security update May 2025. Insight: The flaw exists due to a spoofing vulnerability in .NET Core. Affected systems: .NET Core runtime version 8.0.x prior to

	8.0.16, 9.0.x prior to 9.0.5 and .NET Core SDK version 8.0.x prior to 8.0.409 and 9.0.x prior to 9.0.300. Impact: Successful exploitation allows an attacker to perform spoofing over a network.
CVSS3	8.0
Recommendation	Update .NET Core runtime to version 8.0.16 or 9.0.5 or later and update .NET Core SDK to version 8.0.409 or 9.0.300 or later.
References	Cve: CVE-2025-26646 Url: https://github.com/dotnet/core/blob/main/release-notes/9.0/9.0.5/9.0.5.md Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.16/8.0.16.md Cert-bund: WID-SEC-2025-1015
Affected Nodes	192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 0/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 8.0.11`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 8.0.16 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APSB19-06) - Windows

Severity	▂▃▅▆▇
Description	Adobe Flash Player within Microsoft Edge or Internet Explorer is prone to a remote code execution (RCE) vulnerability. Insight: The flaw exists due to an out-of-bounds read error. Affected systems: Adobe Flash Player prior to 32.0.0.144 within Microsoft Edge or Internet Explorer on, Windows 10 Version 1607 for x32/x64 Edition, Windows 10 Version 1703 for x32/x64 Edition, Windows 10 Version 1709 for x32/x64 Edition, Windows 10 Version 1803 for x32/x64 Edition, Windows 10 Version 1809 for x32/x64 Edition, Windows 10 x32/x64 Edition, Windows 8.1 for x32/x64 Edition, Windows Server 2012/2012 R2, Windows Server 2016 Impact: Successful exploitation allows attackers to conduct information disclosure in the context of the current user.
CVSS3	6.5
Recommendation	Upgrade to Adobe Flash Player 32.0.0.144 or later. Please see the references for more information.
References	Cve: CVE-2019-7090 Url: https://helpx.adobe.com/security/products/flash-player/apsb19-06.html

	Cert-bund: CB-K19/0138
Affected Nodes	192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp

Additional Output	`Vulnerable range:  Less than 32.0.0.144`
	`File checked:      C:\Windows\SysWOW64\Flashplayerapp.exe`
	`File version:      11.8.800.133`

Apache Tomcat Authentication Bypass Vulnerability (Nov 2024) - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to an authentication bypass vulnerability. Insight: If Tomcat was configured to use a custom Jakarta Authentication (formerly JASPIC) ServerAuthContext component which may throw an exception during the authentication process without explicitly setting an HTTP status to indicate failure, the authentication may not have failed, allowing the user to bypass the authentication process. There are no known Jakarta Authentication components that behave in this way. Affected systems: Apache Tomcat versions prior to 9.0.96, 10.0.x through 10.1.30 and 11.0.0-M1 through 11.0.0-M26. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by this flaw. If you disagree with this assessment and want to accept the risk please create an override for this result.
Recommendation	Update to version 9.0.96, 10.1.31, 11.0.0 or later.
References	Cve: CVE-2024-52316 Url: https://lists.apache.org/thread/lopzlqh91jj9n334g02om08sbysdb928 Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.31 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.96 Cert-bund: WID-SEC-2025-0521 Cert-bund: WID-SEC-2024-3684 Cert-bund: WID-SEC-2024-3486
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.96`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat CGI Security Constraint Bypass Vulnerability (May 2025) - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to a CGI security constraint bypass vulnerability. Insight: When running on a case insensitive file system with security constraints configured for the codepathInfo/code component of a URL that mapped to the CGI servlet, it is possible to bypass those security constraints with a specially crafted URL. Affected systems: Apache Tomcat version 9.0.104 and prior, 10.x through 10.1.40 and 11.0.0-M1 through 11.0.6. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.

Recommendation	Update to version 9.0.105, 10.1.41, 11.0.7 or later.
References	Cve: CVE-2025-46701 Url: https://lists.apache.org/thread/xhqqk9w5q45srcdqhogdk04lhdscv30j Cert-bund: WID-SEC-2025-1850 Cert-bund: WID-SEC-2025-1365 Cert-bund: WID-SEC-2025-1165
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp
Additional Output	Installed version: 8.5.71 Fixed version: 9.0.105 Installation path / port: 9443/tcp
Apache Tomcat HTTP/2 Vulnerability (Oct 2020) - Windows	
Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to an information disclosure vulnerability in HTTP/2. Insight: If an HTTP/2 client exceeded the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it is possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers. This could lead to users seeing responses for unexpected resources. Affected systems: Apache Tomcat 8.5.1 to 8.5.57, 9.0.0.M5 to 9.0.37 and 10.0.0-M1 to 10.0.0-M7.
CVSS3	4.3
Recommendation	Update to version 8.5.58, 9.0.38, 10.0.0-M8 or later.
References	Cve: CVE-2020-13943 Url: https://lists.apache.org/thread.html/r4a390027eb27e4550142fac6c8317cc684b157ae314d31514747f307%40%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2023-2467 Cert-bund: CB-K20/0971
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp
Additional Output	Installed version: 9.0.8 Fixed version: 9.0.38 Installation path / port: 1311/tcp
Apache Tomcat HTTP Request Smuggling Vulnerability (Jul 2021) - Windows	
Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to an HTTP request smuggling vulnerability. Insight: Apache Tomcat does not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: Tomcat incorrectly ignores the transfer-encoding header if the client declared it would only accept an HTTP/1.0 response. Tomcat honours the identify encoding and Tomcat does not ensure that, if present, the chunked encoding is the final encoding. Affected systems: Apache Tomcat 8.5.x through 8.5.66, 9.0.0.M1 through 9.0.46 and 10.0.0-M1 through 10.0.6.
CVSS3	5.3
CVE	CVE-2021-33037
Recommendation	Update to version 8.5.68, 9.0.48, 10.0.7 or later.

References	Cve: CVE-2021-33037 Url: https://lists.apache.org/thread.html/r612a79269b0d5e5780c62dfd34286a8037232fec0bc6f1a7e60c9381%40%3Cannounce.tomcat.apache.org%3E Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.7 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.48 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.68 Cert-bund: WID-SEC-2024-2180 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2022-1894 Cert-bund: WID-SEC-2022-1375 Cert-bund: WID-SEC-2022-1296 Cert-bund: WID-SEC-2022-1116 Cert-bund: WID-SEC-2022-0624 Cert-bund: WID-SEC-2022-0623 Cert-bund: WID-SEC-2022-0615 Cert-bund: WID-SEC-2022-0607 Cert-bund: WID-SEC-2022-0094 Cert-bund: CB-K22/0066 Cert-bund: CB-K21/1087 Cert-bund: CB-K21/1084 Cert-bund: CB-K21/0733
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.48`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Information Disclosure Vulnerability (Jan 2021) - Windows

Severity	▮▮▮▯▯
Description	Apache Tomcat is prone to an information disclosure vulnerability. Insight: When serving resources from a network location using the NTFS file system it was possible to bypass security constraints and/or view the source code for JSPs in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances. Affected systems: Apache Tomcat 7.0.0 to 7.0.106, 8.5.0 to 8.5.59, 9.0.0.M1 to 9.0.39 and 10.0.0-M1 to 10.0.0-M9.
CVSS3	5.9
Recommendation	Update to version 7.0.107, 8.5.60, 9.0.40, 10.0.0-M10 or later.
References	Cve: CVE-2021-24122 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.0-M10 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.40 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.60 Url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.107 Url: https://lists.apache.org/thread.html/rce5ac9a40173651d540babce59f6f3825f12c6d4e886ba00823b11e5%40%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2023-2465 Cert-bund: WID-SEC-2022-0607 Cert-bund: CB-K21/0049
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.40`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Information Disclosure Vulnerability (Jan 2024) - Windows	
Severity	▮▮▮▯▯
Description	Apache Tomcat is prone to an information disclosure vulnerability. Insight: Incomplete POST requests triggered an error response that could contain data from a previous request from another user. Affected systems: Apache Tomcat versions 8.5.7 through 8.5.63 and 9.0.0-M11 through 9.0.43.
CVSS3	5.3
Recommendation	Update to version 8.5.64, 9.0.44 or later.
References	Cve: CVE-2024-21733 Url: https://lists.apache.org/thread/h9bjqdd0odj6lhs2o96qgowcc6hb0cfz Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.44 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.64 Cert-bund: WID-SEC-2024-0769 Cert-bund: WID-SEC-2024-0163
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.44`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Information Disclosure Vulnerability (Mar 2023) - Windows	
Severity	▮▮▮▯▯
Description	Apache Tomcat is prone to an information disclosure vulnerability. Insight: When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Tomcat did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel. Affected systems: Apache Tomcat versions through 8.5.85, 9.0.0-M1 through 9.0.71, 10.x through 10.1.5 and 11.0.0-M1 through 11.0.0-M2.
CVSS3	4.3
Recommendation	Update to version 8.5.86, 9.0.72, 10.1.6, 11.0.0-M3 or later.
References	Cve: CVE-2023-28708 Url: https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67 Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M3 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.6 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.72 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.86 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2023-2674 Cert-bund: WID-SEC-2023-1812 Cert-bund: WID-SEC-2023-1808 Cert-bund: WID-SEC-2023-1784 Cert-bund: WID-SEC-2023-1783 Cert-bund: WID-SEC-2023-1782 Cert-bund: WID-SEC-2023-1424 Cert-bund: WID-SEC-2023-1021

	Cert-bund: WID-SEC-2023-1017 Cert-bund: WID-SEC-2023-0717
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     8.5.86`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat JNDI Realm Authentication Weakness Vulnerability (Jul 2021) - Windows

Severity	▮▮▮▯▯
Description	Apache Tomcat is prone to an authentication weakness vulnerability in the JNDI Realm. Insight: Queries made by the JNDI Realm do not always correctly escape parameters. Parameter values could be sourced from user provided data (eg user names) as well as configuration data provided by an administrator. In limited circumstances it is possible for users to authenticate using variations of their user name and/or to bypass some of the protection provided by the LockOut Realm. Affected systems: Apache Tomcat 7.0.x through 7.0.108, 8.5.x through 8.5.65, 9.0.0.M1 through 9.0.45 and 10.0.0-M1 through 10.0.5.
CVSS3	6.5
CVE	CVE-2021-30640
Recommendation	Update to version 7.0.109, 8.5.66, 9.0.46, 10.0.6 or later.
References	Cve: CVE-2021-30640 Url: https://lists.apache.org/thread.html/r59f9ef03929d32120f91f4ea7e6e79edd5688d75d0a9b65fd26d1fe8%40%3Cannounce.tomcat.apache.org%3E Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.0.6 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.46 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.66 Url: https://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.109 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2022-1116 Cert-bund: WID-SEC-2022-0623 Cert-bund: WID-SEC-2022-0615 Cert-bund: WID-SEC-2022-0607 Cert-bund: CB-K21/0733
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.46`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Multiple DoS Vulnerabilities (Mar 2024) - Windows

Severity	▮▮▮▯▯
Description	Apache Tomcat is prone to multiple denial of service (DoS) vulnerabilities. Insight: The following flaws exist: - CVE-2024-23672: WebSocket DoS with incomplete closing handshake

	- CVE-2024-24549: HTTP/2 header handling DoS Affected systems: Apache Tomcat versions prior to 8.5.99, 9.0.0-M1 through 9.0.85, 10.x through 10.1.18 and 11.0.0-M1 through 11.0.0-M16. Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 8.5.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
Recommendation	Update to version 8.5.99, 9.0.86, 10.1.19, 11.0.0-M17 or later.
References	Cve: CVE-2024-23672 Cve: CVE-2024-24549 Url: https://lists.apache.org/thread/cmpswfx6tj4s7x0nxxosvfqs11lvdx2f Url: https://lists.apache.org/thread/4c50rmomhbbsdgfjsgwlb51xdwfjdcvg Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M17 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.19 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.86 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.99 Url: https://nowotarski.info/http2-continuation-flood/ Url: https://nowotarski.info/http2-continuation-flood-technical-details/ Cert-bund: WID-SEC-2024-3663 Cert-bund: WID-SEC-2024-3508 Cert-bund: WID-SEC-2024-3377 Cert-bund: WID-SEC-2024-3220 Cert-bund: WID-SEC-2024-3219 Cert-bund: WID-SEC-2024-3196 Cert-bund: WID-SEC-2024-3195 Cert-bund: WID-SEC-2024-3191 Cert-bund: WID-SEC-2024-1656 Cert-bund: WID-SEC-2024-1642 Cert-bund: WID-SEC-2024-1638 Cert-bund: WID-SEC-2024-1622 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-1214 Cert-bund: WID-SEC-2024-1210 Cert-bund: WID-SEC-2024-0769 Cert-bund: WID-SEC-2024-0630
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.86`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Multiple Vulnerabilities (Dec 2024) - Windows

Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to multiple vulnerabilities. Insight: The following flaws exist: - CVE-2024-50379: Remote code execution (RCE) via write-enabled default servlet - CVE-2024-54677: Denial of service (DoS) in examples web application - CVE-2024-56337: RCE via write-enabled default servlet - CVE-2024-50379 mitigation was incomplete Affected systems: Apache Tomcat versions prior to 9.0.98, 10.x prior to 10.1.34 and 11.x prior to 11.0.2.

	Note: While not explicitly mentioned by the vendor (due to the EOL status of these branches) it is assumed that the whole 10.x branch and all versions prior to 9.x are affected by these flaws. If you disagree with this assessment and want to accept the risk please create an override for this result.
Recommendation	Update to version 9.0.98, 10.1.34, 11.0.2 or later. Vendor note: Users running Tomcat on a case insensitive file system with the default servlet write enabled (readonly initialisation parameter set to the non-default value of false) may need additional configuration to fully mitigate CVE-2024-50379 depending on which version of Java they are using with Tomcat: - running on Java 8 or Java 11: the system property sun.io.useCanonCaches must be explicitly set to false (it defaults to true) - running on Java 17: the system property sun.io.useCanonCaches, if set, must be set to false (it defaults to false) - running on Java 21 onwards: no further configuration is required (the system property and the problematic cache have been removed)
References	Cve: CVE-2024-50379 Cve: CVE-2024-54677 Cve: CVE-2024-56337 Url: https://lists.apache.org/thread/y6lj6q1xnp822g6ro70tn19sgtjmr80r Url: https://lists.apache.org/thread/tdtbbxpg5trdwc2wnopcth9ccvdftq2n Url: https://lists.apache.org/thread/b2b9qrgjrz1kvo4ym8y2wkfdvwoq6qbp Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.2 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.34 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.98 Cert-bund: WID-SEC-2025-0823 Cert-bund: WID-SEC-2025-0819 Cert-bund: WID-SEC-2025-0818 Cert-bund: WID-SEC-2025-0808 Cert-bund: WID-SEC-2025-0719 Cert-bund: WID-SEC-2025-0148 Cert-bund: WID-SEC-2024-3744 Cert-bund: WID-SEC-2024-3722
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     9.0.98`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat 'NIO/NIO2' Connectors Information Disclosure Vulnerability - Windows

Severity	▮▮▮▯▯
Description	Apache Tomcat is prone to an information disclosure vulnerability. Insight: The flaw exists due to an error where a mishandling of close in 'NIO/NIO2' connectors, user sessions can get mixed up. Affected systems: Apache Tomcat 9.0.0.M9 to 9.0.9 Apache Tomcat 8.5.5 to 8.5.31 on Windows. Impact: Successful exploitation can allow an attacker to reuse user sessions in a new connection.
CVSS3	5.9
Recommendation	Upgrade to Apache Tomcat version 9.0.10, 8.5.32 or later. Please see the references for more information.

References	Cve: CVE-2018-8037 Url: http://mail-archives.us.apache.org/mod_mbox/www-announce/201807.mbox/%3C20180722090623.GA92700%40minotaur.apache.org%3E Url: http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.10 Url: http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.32 Cert-bund: WID-SEC-2024-0528 Cert-bund: CB-K19/0921 Cert-bund: CB-K18/1005 Cert-bund: CB-K18/0809
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.10`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Open Redirect Vulnerability (Aug 2023) - Windows	
Severity	▂▃▅▆▇
Description	Apache Tomcat is prone to an open redirect vulnerability. Insight: If the ROOT (default) web application is configured to use FORM authentication then it is possible that a specially crafted URL could be used to trigger a redirect to an URL of the attackers choice. Affected systems: Apache Tomcat versions 8.5.0 through 8.5.92, 9.0.0-M1 through 9.0.79, 10.1.0-M1 through 10.1.12 and 11.0.0-M1 through 11.0.0-M10.
CVSS3	6.1
Recommendation	Update to version 8.5.93, 9.0.80, 10.1.13, 11.0.0-M11 or later.
References	Cve: CVE-2023-41080 Url: https://lists.apache.org/thread/71wvwprtx2j2m54fovq9zr7gbm2wow2f Url: https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.0-M11 Url: https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.13 Url: https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.80 Url: https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.93 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-0871 Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2023-3070 Cert-bund: WID-SEC-2023-2917 Cert-bund: WID-SEC-2023-2690 Cert-bund: WID-SEC-2023-2679 Cert-bund: WID-SEC-2023-2182
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.80`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat Open Redirect Vulnerability - Windows	
Severity	▂▃▅▆▇
Description	When the default servlet in Apache Tomcat returned a redirect to a directory (e.g. redirecting to '/foo/' when the user requested '/foo') a specially crafted URL could be used to cause the redirect to be generated to any URI of the attackers choice.

	Affected systems: Apache Tomcat 9.0.0.M1-9.0.11, 8.5.0-8.5.33, 7.0.23-7.0.90 and probably 8.0.x.
CVSS3	4.3
Recommendation	Update to version 7.0.91, 8.5.34, 9.0.12 or later.
References	Cve: CVE-2018-11784 Url: http://tomcat.apache.org/security-9.html Url: http://tomcat.apache.org/security-8.html Url: http://tomcat.apache.org/security-7.html Cert-bund: WID-SEC-2025-1212 Cert-bund: WID-SEC-2024-1682 Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2023-0531 Cert-bund: WID-SEC-2023-0460 Cert-bund: CB-K20/0029 Cert-bund: CB-K19/1121 Cert-bund: CB-K19/0907 Cert-bund: CB-K19/0616 Cert-bund: CB-K19/0320 Cert-bund: CB-K19/0050 Cert-bund: CB-K18/0963
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.12`
	`Installation`
	`path / port:       1311/tcp`

Apache Tomcat XSS Vulnerability (Jun 2022) - Windows

Severity	📶
Description	Apache Tomcat is prone to a cross-site scripting (XSS) vulnerability. Insight: The Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability. Affected systems: Apache Tomcat version 8.5.50 through 8.5.81, 9.0.30 through 9.0.64, 10.0.0-M1 through 10.0.22 and 10.1.0-M1 through 10.1.0-M16.
CVSS3	6.1
Recommendation	Update to version 8.5.82, 9.0.65, 10.0.23, 10.1.0-M17 or later.
References	Cve: CVE-2022-34305 Url: https://lists.apache.org/thread/k04zk0nq6w57m72w5gb0r6z9ryhmvr4k Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2023-1016 Cert-bund: WID-SEC-2023-0137 Cert-bund: WID-SEC-2022-1782 Cert-bund: WID-SEC-2022-1779 Cert-bund: WID-SEC-2022-1776 Cert-bund: WID-SEC-2022-1767 Cert-bund: WID-SEC-2022-1766 Cert-bund: WID-SEC-2022-0449
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 8.5.71`
	`Fixed version:     8.5.82`
	`Installation`
	`path / port:       9443/tcp`

Apache Tomcat XSS Vulnerability (May 2019) - Windows

Severity	📶
Description	Apache Tomcat is prone to a cross-site scripting vulnerability. Insight: The SSI printenv command in Apache Tomcat echoes user provided data without escaping and is, therefore, vulnerable to XSS. SSI is disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website. Affected systems: Apache Tomcat versions 7.0.0 to 7.0.93, 8.5.0 to 8.5.39 and 9.0.0.M1 to 9.0.17.
CVSS3	6.1
Recommendation	Update to version 7.0.94, 8.5.40, 9.0.18 or later.
References	Cve: CVE-2019-0221 Url: https://seclists.org/fulldisclosure/2019/May/50 Url: https://lists.apache.org/thread.html/6e6e9eacf7b28fd63d249711e9d3ccd4e0a83f556e324aee37be5a8c@%3Cannounce.tomcat.apache.org%3E Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2023-1994 Cert-bund: CB-K20/0029 Cert-bund: CB-K19/0434
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp
Additional Output	Installed version: 9.0.8 Fixed version: 9.0.18 Installation path / port: 1311/tcp

AppleShare IP / Apple Filing Protocol (AFP) Unencrypted Cleartext Login

Severity	📶
Description	The remote host is running a AppleShare IP / Apple Filing Protocol (AFP) service that allows cleartext logins over unencrypted connections. Impact: An attacker can uncover login names and passwords by sniffing traffic to the AppleShare IP / Apple Filing Protocol (AFP) service.
CVSS	4.8
Recommendation	Enable encryption within the service configuration. Please have a look at the manual of the software providing this service for more information on the configuration.
Affected Nodes	192.168.101.200 on port 548/tcp
Additional Output	The following UAMs including the "Cleartxt Passwrd" are reported by the service: DHX2/No User Authent/Cleartxt Passwrd

Backup File Scanner (HTTP) - Unreliable Detection Reporting

Severity	📶
Description	The script reports backup files left on the web server. Insight: 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. Impact: Based on the information provided in these files an attacker might be able to gather sensitive information stored in these files.
Recommendation	Delete the backup files.
References	Url: http://www.openwall.com/lists/oss-security/2017/10/31/1
Affected Nodes	192.168.100.14 on port 80/tcp 192.168.101.5 on port 80/tcp 192.168.101.8 (ilas1nas01.infowerks.com) on port 80/tcp 192.168.101.13 on port 80/tcp

Additional Output	`The following backup files were identified (URL:Matching pattern):`
	
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.backup:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.bak:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.bkp:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.copy:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.old:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.orig:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.save:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.swp:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.temp:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bundle.css.tmp:^HTTP/1\.[01] 200`
	`http://192.168.100.14/ui/.styles.4338f0f38a30dd8dfc28.bu`
	`------------ snipped ------------`

Cleartext Transmission of Sensitive Information via HTTP

Severity	📶
Description	The host / application transmits sensitive information (username, passwords) in cleartext via HTTP. Affected systems: Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection. 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.
CVSS	4.8
Recommendation	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.
References	Url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management Url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure Url: https://cwe.mitre.org/data/definitions/319.html
Affected Nodes	192.168.100.14 on port 80/tcp 192.168.100.18 (ilas3smtp01.infowerks.com) on port 5000/tcp 192.168.101.5 on port 80/tcp 192.168.101.8 (ilas1nas01.infowerks.com) on port 80/tcp 192.168.101.13 on port 80/tcp

Additional Output	`The following input fields were identified (URL:input name):`
	
	`http://192.168.101.5/cs5091759c/config/log_off_page.htm:password$query`

CUPS 2.4.13 Multiple Vulnerabilities

Severity	📶

Description	CUPS is prone to multiple vulnerabilities. Insight: The following flaws exist: - CVE-2025-58060: Authentication bypass with AuthType Negotiate - CVE-2025-58364: Remote DoS via null dereference Affected systems: CUPS prior to version 2.4.13.
Recommendation	Update to version 2.4.13 or later.
References	Cve: CVE-2025-58060 Cve: CVE-2025-58364 Url: https://github.com/OpenPrinting/cups/security/advisories/GHSA-4c68-qgrh-rmmq Url: https://github.com/OpenPrinting/cups/security/advisories/GHSA-7qx3-r744-6qv4 Url: https://github.com/OpenPrinting/cups/releases/tag/v2.4.13 Cert-bund: WID-SEC-2025-2039
Affected Nodes	192.168.101.200 on port 631/tcp

Additional Output	`Installed version: 2.1`
	`Fixed version:     2.4.13`

CUPS 2.4.3 DoS Vulnerability

Severity	▮▮▮▯▯
Description	CUPS is prone to a denial of service (DoS) vulnerability. Insight: A buffer overflow vulnerability in the function format_log_line could allow remote attackers to cause a denial-of-service(DoS) on the affected system. Exploitation of the vulnerability can be triggered when the configuration file cupsd.conf sets the value of loglevel to DEBUG. Affected systems: CUPS prior to version 2.4.3.
CVSS3	5.5
Recommendation	Update to version 2.4.3 or later.
References	Cve: CVE-2023-32324 Url: https://github.com/OpenPrinting/cups/security/advisories/GHSA-cxc6-w2g7-69p7 Url: https://github.com/OpenPrinting/cups/releases/tag/v2.4.3 Cert-bund: WID-SEC-2024-1086 Cert-bund: WID-SEC-2023-2031 Cert-bund: WID-SEC-2023-1349
Affected Nodes	192.168.101.200 on port 631/tcp

Additional Output	`Installed version: 2.1`
	`Fixed version:     2.4.3`

CUPS 2.4.9 File Permission Vulnerability

Severity	▮▮▮▯▯
Description	CUPS is prone to a file permission vulnerability. Insight: When starting the cupsd server with a Listen configuration item pointing to a symbolic link, the cupsd process can be caused to perform an arbitrary chmod of the provided argument, providing world-writable access to the target. Given that cupsd is often running as root, this can result in the change of permission of any user or system files to be world writable. Given the aforementioned Ubuntu AppArmor context, on such systems this vulnerability is limited to those files modifiable by the cupsd process. In that specific case it was found to be possible to turn the configuration of the Listen argument into full control over the cupsd.conf and cups-files.conf configuration files. By later setting the User and Group

	arguments in cups-files.conf, and printing with a printer configured by PPD with a 'FoomaticRIPCommandLine' argument, arbitrary user and group (not root) command execution could be achieved, which can further be used on Ubuntu systems to achieve full root command execution. Affected systems: CUPS prior to version 2.4.9.
CVSS3	6.7
Recommendation	Update to version 2.4.9 or later.
References	Cve: CVE-2024-35235 Url: https://www.openwall.com/lists/oss-security/2024/06/11/1 Url: https://github.com/OpenPrinting/cups/releases/tag/v2.4.9 Cert-bund: WID-SEC-2025-0225 Cert-bund: WID-SEC-2024-1369
Affected Nodes	192.168.101.200 on port 631/tcp

Additional Output	`Installed version: 2.1`
	`Fixed version:     2.4.9`

DCE/RPC and MSRPC Services Enumeration Reporting

Severity	▂▃▅▆▇
Description	Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. Impact: An attacker may use this fact to gain more knowledge about the remote host.
CVSS	5.0
Recommendation	Filter incoming traffic to this ports.
Affected Nodes	192.168.100.18 (ilas3smtp01.infowerks.com) on port 135/tcp 192.168.100.21 (ilas2ftp01.infowerks.com) on port 135/tcp 192.168.100.39 (ILAS1QA03.infowerks.com) on port 135/tcp 192.168.100.54 (ILAS2WKS27.infowerks.com) on port 135/tcp 192.168.100.69 (iwnv-w-wks-judd3.infowerks.com) on port 135/tcp 192.168.100.159 (ILAS3WKS81.infowerks.com) on port 135/tcp 192.168.100.160 (ILAS3WKS82.infowerks.com) on port 135/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 135/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 2103/tcp 192.168.100.165 (ilas1win1003.infowerks.com) on port 135/tcp 192.168.100.170 (ILAS3WKS87.infowerks.com) on port 135/tcp 192.168.100.171 (ILAS3WKS88.infowerks.com) on port 135/tcp 192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 135/tcp 192.168.100.185 (ILAS3WKS95.infowerks.com) on port 135/tcp 192.168.100.200 (ilas3db05.infowerks.com) on port 135/tcp 192.168.101.11 (ilas1bu02.infowerks.com) on port 135/tcp 192.168.101.14 (ilas1dc03.infowerks.com) on port 135/tcp 192.168.101.15 (ilas1fs02.infowerks.com) on port 135/tcp 192.168.101.32 (ilas1fs01.infowerks.com) on port 135/tcp 192.168.101.63 (imike.infowerks.com) on port 135/tcp 192.168.101.66 (ilas1sql02.infowerks.com) on port 135/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 135/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 135/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 135/tcp 192.168.101.85 (ilas3wks04.infowerks.com) on port 135/tcp 192.168.101.88 (ilas1sql04.infowerks.com) on port 135/tcp 192.168.101.111 (ilas1dc01.infowerks.com) on port 135/tcp 192.168.101.112 (icage0dc02.infowerks.com) on port 135/tcp 192.168.101.122 (ILAS1DRN12.infowerks.com) on port 135/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 135/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 135/tcp 192.168.101.141 (ILAS1WKS09.infowerks.com) on port 135/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 135/tcp

	192.168.101.155 (ilas1iruntst1.infowerks.com) on port 135/tcp 192.168.101.159 (iwnv-w-wks-lvillegas.infowerks.com) on port 135/tcp 192.168.101.160 (iwnv-w-wks-vminnick.infowerks.com) on port 135/tcp 192.168.101.175 (iSQL1.infowerks.com) on port 135/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 135/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 135/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 135/tcp 192.168.101.184 (ilas3db140.infowerks.com) on port 135/tcp 192.168.101.185 (ilas3stor01.infowerks.com) on port 135/tcp 192.168.101.186 (ilas3db154.infowerks.com) on port 135/tcp 192.168.101.187 (ilas2db10.infowerks.com) on port 135/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 135/tcp 192.168.101.192 (ILAS3DB160.infowerks.com) on port 135/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 135/tcp 192.168.101.194 (ilas1win1004.infowerks.com) on port 135/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 135/tcp 192.168.101.198 (ILAS2IMG16.infowerks.com) on port 135/tcp 192.168.101.205 (ilas1as04.infowerks.com) on port 135/tcp 192.168.101.206 (ILAS4BCC2.infowerks.com) on port 135/tcp 192.168.101.221 (ilas1as09.infowerks.com) on port 135/tcp 192.168.101.232 (ILAS2IMG15.infowerks.com) on port 135/tcp 192.168.101.254 (ilas2fs05.infowerks.com) on port 135/tcp 192.168.101.254 (ilas2fs05.infowerks.com) on port 2103/tcp 192.168.199.22 on port 135/tcp 192.168.199.40 on port 135/tcp 192.168.199.89 on port 135/tcp 192.168.199.90 on port 135/tcp 192.168.101.254 (ilas2fs05.infowerks.com) on port 2107/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 1587/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 1541/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 1536/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 1537/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 1572/tcp 192.168.101.254 (ilas2fs05.infowerks.com) on port 2105/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 1542/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 1538/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 1540/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 1539/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 2105/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 2107/tcp

Additional Output

```
The following DCE/RPC or MSRPC services are running on this port:

     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.101.84[1540]

     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.101.84[1540]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service

     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.101.84[1540]

     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.101.84[1540]

     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.101.84[1540]
```

Dell OpenManage Server Administrator Directory Traversal Vulnerability (Apr 2016)

Severity	▮▮▮▯▯

Description	Dell OpenManage Server Administrator is prone to a directory traversal vulnerability. Insight: The flaw is due to insufficient validation of user supplied input via 'file' parameter to ViewFile. Affected systems: Dell OpenManage Server Administrator version 8.4 and prior. Impact: Successful exploitation will allow remote authenticated administrators to read arbitrary files on the affected system.
CVSS3	4.9
Recommendation	Update to version 8.5 or later.
References	Cve: CVE-2016-4004 Url: https://dl.dell.com/topicspdf/omsa-oms-8-4-cve_rn_en-us.pdf Url: https://www.exploit-db.com/exploits/39486
Affected Nodes	192.168.101.254 (ilas2fs05.infowerks.com) on port 1311/tcp

Additional Output	`Installed version: 8.2.0`
	`Fixed version:     8.5`
	`Installation`
	`path / port:       /`

.NET Core Denial of Service Vulnerability (Jun 2021)

Severity	▮▮▮▯▯
Description	ASP.NET Core is prone to a denial of service vulnerability. Insight: The flaw exists due to an unspecified error in the Microsoft ASP.NET Core Affected systems: ASP.NET Core version 5.0 and 3.1 Impact: Successful exploitation will allow an attacker to conduct a denial of service attack on the affected system.
CVSS3	5.9
Recommendation	The vendor has released updates. Please see the references for more information.
References	Cve: CVE-2021-31957 Url: https://github.com/dotnet/core/blob/main/release-notes/5.0/5.0.7/5.0.7.md Url: https://github.com/dotnet/core/blob/main/release-notes/3.1/3.1.16/3.1.16.md Url: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31957 Cert-bund: CB-K21/0624
Affected Nodes	192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.192 (ILAS3DB160.infowerks.com) on port 0/tcp 192.168.101.186 (ilas3db154.infowerks.com) on port 0/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 0/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 5.0`
	`Fixed version:     5.0.7`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Information Disclosure Vulnerabilities - Windows

Severity	▮▮▮▯▯
Description	.NET Core and is prone to an information disclosure vulnerability. Insight: The flaw is due to incorrect processing of user-supplied data in .NET. Affected systems: .NET Core runtime 6.0 before 6.0.8, 3.1 before 3.1.28 and .NET Core SDK before 6.0.108, 3.1 before 3.1.422. Impact: Successful exploitation will allow an attacker to disclose sensitive information and allow to spoof page content.
CVSS3	5.9
Recommendation	Upgrade .NET Core runtimes to versions 6.0.8 or 3.1.28 or later or upgrade .NET Core SDK to versions 6.0.108 or 6.0.303 or 6.0.400 or 3.1.422 or later.
References	Cve: CVE-2022-34716 Url: https://github.com/dotnet/core/blob/main/release-notes/6.0/6.0.8/6.0.8.md Url: https://github.com/dotnet/core/blob/main/release-notes/3.1/3.1.28/3.1.28.md Cert-bund: WID-SEC-2022-0954
Affected Nodes	192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 3.1.6`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 3.1.28 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Information Disclosure Vulnerability (KB5015424)

Severity	▮▮▮▯▯
Description	This host is missing an important security update according to Microsoft KB5015424. Insight: The flaw is due to an excessive data output by the application in .NET. Affected systems: .NET Core versions 3.1 prior to 3.1.26, 6.0 prior to 6.0.6. Impact: Successful exploitation will allow an attacker to gain unauthorized access to sensitive information on the system.
CVSS3	5.5
Recommendation	Upgrade .NET Core to version 3.1.26 or 6.0.6 or later.
References	Cve: CVE-2022-30184 Url: https://github.com/dotnet/core/blob/main/release-notes/6.0/6.0.6/6.0.6.md Url: https://github.com/dotnet/core/blob/main/release-notes/3.1/3.1.26/3.1.26.md Cert-bund: WID-SEC-2022-0327
Affected Nodes	192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp

	192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 3.1.6`
	`Fixed version:     3.1.26`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Multiple Vulnerabilities (KB5038351)

Severity	▁▃▅▇
Description	This host is missing an important security update according to Microsoft KB5038351. Insight: These vulnerabilities exist: - CVE-2024-30045: .NET Remote Code Execution Vulnerability - CVE-2024-30046: .NET Denial of Service Vulnerability Affected systems: .NET Core runtime 7.x before 7.0.19, 8.x before 8.0.5 and .NET Core SDK 7.x before 7.0.409, 8.x before 8.0.300. Impact: Successful exploitation allows an attacker to execute arbitrary commands and conduct denial of service attacks.
CVSS3	6.3
Recommendation	Update .NET Core runtime to version 7.0.19 or 8.0.5 or later or update .NET Core SDK to version 7.0.409 or 8.0.300 later.
References	Cve: CVE-2024-30045 Cve: CVE-2024-30046 Url: https://github.com/dotnet/core/blob/main/release-notes/7.0/7.0.19/7.0.19.md Url: https://github.com/dotnet/core/blob/main/release-notes/8.0/8.0.5/8.0.5.md Cert-bund: WID-SEC-2024-1115
Affected Nodes	192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp

Additional Output	`Installed version: ASP .NET Core With Microsoft .NET Core runtimes 8.0.3`
	`Fixed version:     ASP .NET Core With Microsoft .NET Core runtimes version 7.0.19 or 8.0.5 or later`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core SDK Spoofing Vulnerability (Feb 2019)

Severity	▁▃▅▇
Description	ASP.NET Core SDK is prone to a spoofing vulnerability. Insight: The flaw exists due to an error in .Net Framework API's in the way they parse URL's. Affected systems: ASP.NET Core SDK 1.x prior to version 1.1.12, 2.1.x prior to version 2.1.504 and 2.2.x prior to version 2.2.104 Impact: Successful exploitation will allow an attacker to conduct spoofing attacks.
CVSS3	5.9
Recommendation	Upgrade to ASP.NET Core SDK 1.1.12 or 2.1.504 or 2.2.104 or later.

References	Cve: CVE-2019-0657 Url: https://github.com/dotnet/core/blob/master/release-notes/2.2/2.2.2/2.2.2.md Url: http://www.securityfocus.com/bid/106890 Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.8/2.1.8.md Url: https://github.com/dotnet/core/blob/master/release-notes/1.1/1.1.11/1.1.11.md Url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0657 Cert-bund: CB-K19/0136 Cert-bund: CB-K19/0135
Affected Nodes	192.168.101.186 (ilas3db154.infowerks.com) on port 0/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.500`
	`Fixed version:     2.1.504`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core SDK Spoofing Vulnerability (Jul 2019)

Severity	▮▮▮▯▯
Description	ASP.NET Core SDK is prone to spoofing vulnerability. Insight: The flaw exists due to an error in ASP.NET Core that could lead to an open redirect. Affected systems: ASP.NET Core SDK 2.1.x prior to version 2.1.508 and 2.2.x prior to version 2.2.108 Impact: Successful exploitation will allow an attacker to conduct Spoofing attack.
CVSS3	6.1
Recommendation	Upgrade to ASP.NET Core SDK 2.1.508 or 2.2.108 or later.
References	Cve: CVE-2019-1075 Url: https://github.com/dotnet/core/blob/master/release-notes/2.2/2.2.6/2.2.6.md Url: http://www.securityfocus.com/bid/108984 Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.12/2.1.12.md Url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1075 Cert-bund: CB-K19/0593
Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.500`
	`Fixed version:     2.1.508`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Spoofing Vulnerability (Feb 2019)

Severity	▮▮▮▯▯
Description	ASP.NET Core is prone to a spoofing vulnerability. Insight: The flaw exists due to an error in .Net Framework API's in the way they parse URL's. Affected systems: ASP.NET Core 1.0.x prior to version 1.0.14, 1.1.x prior to version 1.1.11, 2.1.x prior to version 2.1.8 and 2.2.x prior to version 2.2.2

	Impact: Successful exploitation will allow an attacker to conduct spoofing attacks.
CVSS3	5.9
Recommendation	Upgrade to ASP.NET Core 1.0.14 or 1.1.11 or 2.1.8 or 2.2.2 or later.
References	Cve: CVE-2019-0657 Url: https://github.com/dotnet/core/blob/master/release-notes/2.2/2.2.2/2.2.2.md Url: http://www.securityfocus.com/bid/106890 Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.8/2.1.8.md Url: https://github.com/dotnet/core/blob/master/release-notes/1.1/1.1.11/1.1.11.md Url: https://github.com/dotnet/core/blob/master/release-notes/1.0/1.0.14/1.0.14.md Url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0657 Cert-bund: CB-K19/0136 Cert-bund: CB-K19/0135
Affected Nodes	192.168.101.186 (ilas3db154.infowerks.com) on port 0/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.6`
	`Fixed version:     2.1.8`
	`Installation`
	`path / port:       Could not find the install location from registry`

.NET Core Spoofing Vulnerability (Jul 2019)

Severity	▮▮▮▯▯
Description	ASP.NET Core is prone to spoofing vulnerability. Insight: The flaw exists due to an error in ASP.NET Core that could lead to an open redirect. Affected systems: ASP.NET Core 2.1.x prior to version 2.1.12 and 2.2.x prior to version 2.2.6 Impact: Successful exploitation will allow an attacker to conduct Spoofing attack.
CVSS3	6.1
Recommendation	Upgrade to ASP.NET Core SDK 2.1.12 or 2.2.6 or later.
References	Cve: CVE-2019-1075 Url: https://github.com/dotnet/core/blob/master/release-notes/2.2/2.2.6/2.2.6.md Url: http://www.securityfocus.com/bid/108984 Url: https://github.com/dotnet/core/blob/master/release-notes/2.1/2.1.12/2.1.12.md Url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1075 Cert-bund: CB-K19/0593
Affected Nodes	192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 2.1.6`
	`Fixed version:     2.1.12`
	`Installation`
	`path / port:       Could not find the install location from registry`

7-Zip Arbitrary File Write Vulnerability (Oct 2025) - Windows

Severity	▮▮▯▯▯
Description	7zip is prone to an arbitrary file write vulnerability.

	Affected systems: 7zip prior to version 25.01 on Windows. Impact: Successful exploitation allows an attacker to perform arbitrary file writes on target systems.
Recommendation	Update to version 25.01 or later.
References	Cve: CVE-2025-55188 Url: https://www.7-zip.org/history.txt Url: https://lunbun.dev/blog/cve-2025-55188/ Cert-bund: WID-SEC-2025-1750
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp 192.168.101.206 (ILAS4BCC2.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 24.08`
	`Fixed version:     25.01`
	`Installation`
	`path / port:       Unable to find the install location`

7-Zip Multiple Vulnerabilities (Apr 2025) - Windows

Severity	▮▮▯▯▯
Description	7zip is prone to multiple vulnerabilities. Affected systems: 7zip version 22.01 and prior on Windows. Impact: Successful exploitation allows an attacker to conduct denial of service attacks.
CVSS3	3.3
Recommendation	No known solution is available as of 23th April, 2025. Information regarding this issue will be updated once solution details are available.
References	Cve: CVE-2022-47111 Cve: CVE-2022-47112 Url: https://github.com/boofish/semantic-bugs/
Affected Nodes	192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp

Additional Output	`Installed version: 9.20`
	`Fixed version:     None`
	`Installation`
	`path / port:       Unable to find the install location`

Apache Tomcat Information Disclosure Vulnerability (Sep 2022) - Windows

Severity	▮▮▯▯▯
Description	Apache Tomcat is prone to an information disclosure vulnerability. Insight: The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug that could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client. Affected systems: Apache Tomcat version 8.5.0 through 8.5.77, 9.0.0-M1 through 9.0.60, 10.0.0-M1 through 10.0.18 and 10.1.0-M1 through 10.1.0-M12.
CVSS3	3.7
Recommendation	Update to version 8.5.78, 9.0.62, 10.0.20, 10.1.0-M14 or later.

References	Cve: CVE-2021-43980 Url: https://lists.apache.org/thread/3jjqbsp6j88b198x5rmg99b1qr8ht3g3 Cert-bund: WID-SEC-2024-1238 Cert-bund: WID-SEC-2024-0528 Cert-bund: WID-SEC-2022-1558
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp

Additional Output	`Installed version: 9.0.8`
	`Fixed version:     9.0.62`
	`Installation`
	`path / port:       1311/tcp`

7zip Detection (Windows SMB Login)

Severity	▮▯▯▯▯
Description	Detects the installed version of 7zip on Windows. The script logs in via smb, searches for 7zip in the registry and gets the version from 'DisplayName' string in registry.

<table>
<tr><td>Affected Nodes</td><td>192.168.100.171 (ILAS3WKS88.infowerks.com) on port 0/tcp
192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp
192.168.100.39 (ILAS1QA03.infowerks.com) on port 0/tcp
192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp
192.168.100.164 (ilas1win1002.infowerks.com) on port 0/tcp
192.168.101.191 (ILAS2PG01.infowerks.com) on port 0/tcp
192.168.101.232 (ILAS2IMG15.infowerks.com) on port 0/tcp
192.168.101.159 (iwnv-w-wks-lvillegas.infowerks.com) on port 0/tcp
192.168.101.205 (ilas1as04.infowerks.com) on port 0/tcp
192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp
192.168.101.85 (ilas3wks04.infowerks.com) on port 0/tcp
192.168.100.200 (ilas3db05.infowerks.com) on port 0/tcp
192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp
192.168.100.159 (ILAS3WKS81.infowerks.com) on port 0/tcp
192.168.100.21 (ilas2ftp01.infowerks.com) on port 0/tcp
192.168.100.160 (ILAS3WKS82.infowerks.com) on port 0/tcp
192.168.100.69 (iwnv-w-wks-judd3.infowerks.com) on port 0/tcp
192.168.101.192 (ILAS3DB160.infowerks.com) on port 0/tcp
192.168.101.186 (ilas3db154.infowerks.com) on port 0/tcp
192.168.101.196 (ilas3db153.infowerks.com) on port 0/tcp
192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 0/tcp
192.168.100.185 (ILAS3WKS95.infowerks.com) on port 0/tcp
192.168.101.160 (iwnv-w-wks-vminnick.infowerks.com) on port 0/tcp
192.168.101.184 (ilas3db140.infowerks.com) on port 0/tcp
192.168.101.122 (ILAS1DRN12.infowerks.com) on port 0/tcp
192.168.101.254 (ilas2fs05.infowerks.com) on port 0/tcp
192.168.101.198 (ILAS2IMG16.infowerks.com) on port 0/tcp
192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp
192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp
192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp
192.168.101.206 (ILAS4BCC2.infowerks.com) on port 0/tcp
192.168.100.54 (ILAS2WKS27.infowerks.com) on port 0/tcp
192.168.101.141 (ILAS1WKS09.infowerks.com) on port 0/tcp
192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp
192.168.101.193 (ILAS3DB162.infowerks.com) on port 0/tcp
192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp
192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp
192.168.101.175 (iSQL1.infowerks.com) on port 0/tcp
192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp
192.168.101.221 (ilas1as09.infowerks.com) on port 0/tcp
192.168.101.185 (ilas3stor01.infowerks.com) on port 0/tcp
192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp</td></tr>
<tr><td>Additional Output</td><td><pre>
Detected 7-Zip 9.20 (x64 edition)

Version: 9.20
Location: Unable to find the install location
CPE: cpe:/a:7-zip:7-zip:x64:9.20

Concluded from version/product identification result:
9.20
</pre></td></tr>
<tr><td colspan="2"><b>Adobe Flash Player Within Microsoft IE and Edge Detection (Windows SMB Login)</b></td></tr>
<tr><td>Severity</td><td>▮▯▯▯▯</td></tr>
<tr><td>Description</td><td>SMB login-based detection of Adobe Flash Player within Microsoft Internet Explorer (IE) and Edge.</td></tr>
<tr><td>Affected Nodes</td><td>192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp
192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp
192.168.101.192 (ILAS3DB160.infowerks.com) on port 0/tcp
192.168.101.184 (ilas3db140.infowerks.com) on port 0/tcp
192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp
192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp</td></tr>
</table>

<table>
<tr><td></td><td>192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp
192.168.101.185 (ilas3stor01.infowerks.com) on port 0/tcp</td></tr>
<tr><td>Additional Output</td><td><pre>
Detected Adobe Flash Player within IE/Edge

Version: 32.0.0.255
Location: C:\WINDOWS\SysWOW64
CPE: cpe:/a:adobe:flash_player_internet_explorer:32.0.0.255

Concluded from version/product identification result:
32.0.0.255
</pre></td></tr>
</table>

Adobe Products Detection (Windows SMB Login)

<table>
<tr><td>Severity</td><td>▮▯▯▯▯</td></tr>
<tr><td>Description</td><td>Detects the installed version of Adobe Products.

The script logs in via smb, searches for Adobe Products in the registry and gets the version from 'DisplayVersion' string in registry.</td></tr>
<tr><td>Affected Nodes</td><td>192.168.100.171 (ILAS3WKS88.infowerks.com) on port 0/tcp
192.168.100.39 (ILAS1QA03.infowerks.com) on port 0/tcp
192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp
192.168.101.232 (ILAS2IMG15.infowerks.com) on port 0/tcp
192.168.100.159 (ILAS3WKS81.infowerks.com) on port 0/tcp
192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 0/tcp
192.168.100.185 (ILAS3WKS95.infowerks.com) on port 0/tcp
192.168.101.198 (ILAS2IMG16.infowerks.com) on port 0/tcp
192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp
192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp</td></tr>
<tr><td>Additional Output</td><td><pre>
Detected Adobe Acrobat (64-bit)

Version: 25.001.20844
Location: C:\Program Files\Adobe\Acrobat DC\
CPE: cpe:/a:adobe:acrobat:25.001.20844

Concluded from version/product identification result:
25.001.20844
</pre></td></tr>
</table>

Allowed HTTP Methods Enumeration

<table>
<tr><td>Severity</td><td>▮▯▯▯▯</td></tr>
<tr><td>Description</td><td>Enumerates which HTTP methods are allowed.

Insight: - Basic HTTP methods: GET, HEAD, POST, PUT, DELETE, CONNECT,
OPTIONS, TRACE

- Extended HTTP methods: ACL, BASELINE-CONTROL, BIND, CHECKIN, CHECKOUT, COPY, LABEL, LINK, LOCK,
MERGE, MKACTIVITY, MKCALENDAR, MKCOL, MKREDIRECTREF, MKWORKSPACE, MOVE, ORDERPATCH, PATCH, PRI,
PROPFIND, PROPPATCH, REBIND, REPORT, SEARCH, UNBIND, UNCHECKOUT, UNLINK, UNLOCK, UPDATE, UPDATEREDIRECTREF, VERSION-CONTROL</td></tr>
<tr><td>Affected Nodes</td><td>192.168.100.14 on port 80/tcp
192.168.100.18 (ilas3smtp01.infowerks.com) on port 80/tcp
192.168.100.18 (ilas3smtp01.infowerks.com) on port 5000/tcp
192.168.100.164 (ilas1win1002.infowerks.com) on port 80/tcp
192.168.100.164 (ilas1win1002.infowerks.com) on port 5000/tcp
192.168.100.165 (ilas1win1003.infowerks.com) on port 5000/tcp
192.168.101.3 on port 80/tcp
192.168.101.5 on port 80/tcp
192.168.101.6 on port 80/tcp</td></tr>
</table>

```
192.168.101.6 on port 443/tcp
192.168.101.6 on port 5989/tcp
192.168.101.8 (ilas1nas01.infowerks.com) on port 80/tcp
192.168.101.12 on port 443/tcp
192.168.101.13 on port 80/tcp
192.168.101.14 (ilas1dc03.infowerks.com) on port 5000/tcp
192.168.101.15 (ilas1fs02.infowerks.com) on port 5000/tcp
192.168.101.17 (ilas1sw01.infowerks.com) on port 80/tcp
192.168.101.17 (ilas1sw01.infowerks.com) on port 443/tcp
192.168.101.17 (ilas1sw01.infowerks.com) on port 5989/tcp
192.168.101.24 on port 443/tcp
192.168.101.26 (ilas1qa02.infowerks.com) on port 80/tcp
192.168.101.26 (ilas1qa02.infowerks.com) on port 443/tcp
192.168.101.26 (ilas1qa02.infowerks.com) on port 5989/tcp
192.168.101.29 (db-details.infowerks.com) on port 80/tcp
192.168.101.29 (db-details.infowerks.com) on port 443/tcp
192.168.101.29 (db-details.infowerks.com) on port 5000/tcp
192.168.101.32 (ilas1fs01.infowerks.com) on port 5000/tcp
192.168.101.39 on port 80/tcp
192.168.101.39 on port 443/tcp
192.168.101.39 on port 5989/tcp
192.168.101.50 on port 5000/tcp
192.168.101.51 (ilas1drn01.infowerks.com) on port 80/tcp
192.168.101.63 (imike.infowerks.com) on port 5000/tcp
192.168.101.66 (ilas1sql02.infowerks.com) on port 5000/tcp
192.168.101.69 (ilas1as14.infowerks.com) on port 443/tcp
192.168.101.69 (ilas1as14.infowerks.com) on port 5000/tcp
192.168.101.69 (ilas1as14.infowerks.com) on port 9443/tcp
192.168.101.88 (ilas1sql04.infowerks.com) on port 5000/tcp
192.168.101.91 (archive.infowerks.com) on port 9090/tcp
192.168.101.92 on port 5000/tcp
192.168.101.93 (ilas1db04.infowerks.com) on port 5000/tcp
192.168.101.111 (ilas1dc01.infowerks.com) on port 5000/tcp
192.168.101.112 (icage0dc02.infowerks.com) on port 5000/tcp
192.168.101.114 on port 80/tcp
192.168.101.154 (ilas3wks46.infowerks.com) on port 5000/tcp
192.168.101.175 (iSQL1.infowerks.com) on port 5000/tcp
192.168.101.180 (ilas3db142.infowerks.com) on port 5000/tcp
192.168.101.181 (ILAS3DB161.infowerks.com) on port 5000/tcp
192.168.101.184 (ilas3db140.infowerks.com) on port 5000/tcp
192.168.101.185 (ilas3stor01.infowerks.com) on port 80/tcp
192.168.101.185 (ilas3stor01.infowerks.com) on port 5000/tcp
192.168.101.186 (ilas3db154.infowerks.com) on port 5000/tcp
192.168.101.187 (ilas2db10.infowerks.com) on port 5000/tcp
192.168.101.189 on port 5000/tcp
192.168.101.191 (ILAS2PG01.infowerks.com) on port 5000/tcp
192.168.101.192 (ILAS3DB160.infowerks.com) on port 80/tcp
192.168.101.192 (ILAS3DB160.infowerks.com) on port 5000/tcp
192.168.101.193 (ILAS3DB162.infowerks.com) on port 5000/tcp
192.168.101.194 (ilas1win1004.infowerks.com) on port 5000/tcp
192.168.101.196 (ilas3db153.infowerks.com) on port 5000/tcp
192.168.101.200 on port 80/tcp
192.168.101.200 on port 631/tcp
192.168.101.208 (ilas2db07.infowerks.com) on port 443/tcp
192.168.101.215 on port 80/tcp
192.168.101.216 on port 80/tcp
192.168.101.221 (ilas1as09.infowerks.com) on port 80/tcp
192.168.101.221 (ilas1as09.infowerks.com) on port 443/tcp
192.168.101.221 (ilas1as09.infowerks.com) on port 5000/tcp
192.168.101.221 (ilas1as09.infowerks.com) on port 8088/tcp
192.168.101.221 (ilas1as09.infowerks.com) on port 10080/tcp
192.168.101.225 on port 80/tcp
192.168.101.254 (ilas2fs05.infowerks.com) on port 80/tcp
192.168.199.6 on port 443/tcp
192.168.199.6 on port 5989/tcp
192.168.199.74 on port 443/tcp
```

	192.168.199.78 on port 443/tcp 192.168.101.221 (ilas1as09.infowerks.com) on port 8084/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 8084/tcp 192.168.101.12 on port 3033/tcp 192.168.101.24 on port 3033/tcp 192.168.101.53 (ilas1drn03.infowerks.com) on port 3232/tcp

Additional Output

```
The following list contains the URLs and corresponding supported HTTP methods.

URL                    | HTTP Methods
-------------------------------------
https://192.168.199.6/ | GET,HEAD
```

Anti-Scanner Defenses (HTTP)

Severity	▂▃▅▆▇
Description	It seems that the remote web server rejects HTTP requests from the Scanner. It is probably protected by a reverse proxy, WAF or IDS/IPS.
CVSS	0.0
Recommendation	Whitelist the IP of the scanner to e.g. not block/reject HTTP requests done by scanner for accurate audit/scan results.
Affected Nodes	192.168.199.5 on port 80/tcp 192.168.199.6 on port 80/tcp 192.168.199.22 on port 80/tcp 192.168.199.22 on port 47001/tcp 192.168.199.40 on port 47001/tcp 192.168.199.74 on port 80/tcp 192.168.199.78 on port 80/tcp 192.168.199.89 on port 47001/tcp 192.168.199.90 on port 5000/tcp 192.168.199.90 on port 47001/tcp

Additional Output

```
By sending a different User-Agent the remote web server is answering with different HTTP responses:

1. Status Code : 404
1. User-Agent  : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
ome/51.0.2704.79 Safari/537.36 Edge/14.14393
2. Status Code : No response (probably blocked)
2. User-Agent  : Mozilla/5.0 [en] (X11, U; OpenVAS-VT 23.20.1)
```

AnyDesk Desktop Detection Consolidation

Severity	▂▃▅▆▇
Description	Consolidation of AnyDesk Desktop detections.
References	Url: https://anydesk.com
Affected Nodes	192.168.101.141 (ILAS1WKS09.infowerks.com) on port 0/tcp

Additional Output

```
Detected AnyDesk Desktop

Version:       9.0.9
Location:      /
CPE:           cpe:/a:anydesk:anydesk:9.0.9

Concluded from:
- Local Detection over SMB
  Concluded from version/product identification result:
    Registry Key:    SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk
    DisplayName:     AnyDesk
    DisplayVersion: ad 9.0.9
    Location:        "C:\Program Files\AnyDesk"
```

Apache HTTP Server Detection Consolidation

Severity	▮▯▯▯▯
Description	Consolidation of Apache HTTP Server detections.
References	Url: https://httpd.apache.org
Affected Nodes	192.168.101.24 on port 0/tcp 192.168.101.12 on port 0/tcp

Additional Output

```
Detected Apache HTTP Server

Version:       unknown
Location:      3033/tcp
CPE:           cpe:/a:apache:http_server

Concluded from version/product identification result:
Server: Apache

Detected Apache HTTP Server

Version:       unknown
Location:      443/tcp
CPE:           cpe:/a:apache:http_server

Concluded from version/product identification result:
Server: Apache

Detected Apache HTTP Server

Version:       unknown
Location:      80/tcp
CPE:           cpe:/a:apache:http_server

Concluded from version/product identification result:
Server: Apache
```

Apache Tomcat Detection Consolidation

Severity	▮▯▯▯▯
Description	Consolidation of Apache Tomcat detections.
CVSS	0.0
References	Url: http://tomcat.apache.org/
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 0/tcp

Additional Output

```
Detected Apache Tomcat

Version:       9.0.8
Location:      1311/tcp
CPE:           cpe:/a:apache:tomcat:9.0.8

Concluded from version/product identification result:
Apache Tomcat/9.0.8

Concluded from version/product identification location:
https://ilas1as14.infowerks.com:1311/[

Detected Apache Tomcat

Version:       8.5.71
Location:      9443/tcp
CPE:           cpe:/a:apache:tomcat:8.5.71

Concluded from version/product identification result:
```

```
Apache Tomcat/8.5.71

Concluded from version/product identification location:
https://ilas1as14.infowerks.com:9443/[
```

Apple / OpenPrinting CUPS Detection (HTTP)

Severity	▮▯▯▯▯
Description	HTTP based detection of Common Unix Printing System (CUPS).
References	Url: https://www.cups.org/ Url: https://openprinting.github.io/cups
Affected Nodes	192.168.101.200 on port 631/tcp

Additional Output

```
Detected Apple / OpenPrinting CUPS

Version:       2.1
Location:      /
CPE:           cpe:/a:apple:cups:2.1

Concluded from version/product identification result:
  Server: CUPS/2.1 IPP/2.1

Concluded from version/product identification location:
http://192.168.101.200:631/
```

AppleShare IP / Apple Filing Protocol (AFP) Service Detection

Severity	▮▯▯▯▯
Description	The remote host is running an AppleShare IP / Apple Filing Protocol (AFP) service. By sending a DSIGetStatus request on tcp port 548, it was possible to disclose information about the remote host.
CVSS	0.0
Affected Nodes	192.168.101.200 on port 548/tcp

Additional Output

```
This host is running an AppleShare IP / Apple Filing Protocol (AFP) service.

Machine type: Netatalk3.1.9.q1
Server name:  QNAPDataStore
UAMs:         DHX2/No User Authent/Cleartxt Passwrd
AFP Versions: AFP2.2/AFPX03/AFP3.1/AFP3.2/AFP3.3/AFP3.4

The remote service allows the "guest" user to connect.
The remote service allows "Cleartext" connections.
```

ASP.NET Core/.NET Core SDK Detection (Windows SMB Login)

Severity	▮▯▯▯▯
Description	Detects the installed version of ASP.NET Core. The script logs in via smb, searches for 'Microsoft .NET Core in the registry and gets the version from 'DisplayName' string from registry.
Affected Nodes	192.168.100.171 (ILAS3WKS88.infowerks.com) on port 0/tcp 192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 0/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp

	192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.192 (ILAS3DB160.infowerks.com) on port 0/tcp 192.168.101.186 (ilas3db154.infowerks.com) on port 0/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 0/tcp 192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 0/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp 192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp

Additional Output

```
Detected .NET Core SDK

Version:       2.1.526
Location:      Could not find the install location from registry
CPE:           cpe:/a:microsoft:.netcore_sdk:x64:2.1.526

Concluded from version/product identification result:
.NET Core SDK 2.1.526
```

Authenticated Scan / LSC Info Consolidation (Windows SMB Login)

Severity	▮▯▯▯▯
Description	Consolidation and reporting of various technical information about authenticated scans / local security checks (LSC) via SMB for Windows targets.
CVSS	0.0
References	Url: https://docs.greenbone.net/GSM-Manual/gos-24.10/en/scanning.html#requirements-on-target-systems-with-microsoft-windows Url: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/scanning.html#requirements-on-target-systems-with-microsoft-windows
Affected Nodes	192.168.101.32 (ilas1fs01.infowerks.com) on port 0/tcp 192.168.199.40 on port 0/tcp 192.168.100.171 (ILAS3WKS88.infowerks.com) on port 0/tcp 192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.101.14 (ilas1dc03.infowerks.com) on port 0/tcp 192.168.199.89 on port 0/tcp 192.168.100.39 (ILAS1QA03.infowerks.com) on port 0/tcp 192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.199.22 on port 0/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 0/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 0/tcp 192.168.101.112 (icage0dc02.infowerks.com) on port 0/tcp 192.168.101.232 (ILAS2IMG15.infowerks.com) on port 0/tcp 192.168.101.159 (iwnv-w-wks-lvillegas.infowerks.com) on port 0/tcp 192.168.101.205 (ilas1as04.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.85 (ilas3wks04.infowerks.com) on port 0/tcp 192.168.100.200 (ilas3db05.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.66 (ilas1sql02.infowerks.com) on port 0/tcp 192.168.101.11 (ilas1bu02.infowerks.com) on port 0/tcp 192.168.100.159 (ILAS3WKS81.infowerks.com) on port 0/tcp 192.168.100.21 (ilas2ftp01.infowerks.com) on port 0/tcp 192.168.100.160 (ILAS3WKS82.infowerks.com) on port 0/tcp 192.168.100.69 (iwnv-w-wks-judd3.infowerks.com) on port 0/tcp 192.168.101.192 (ILAS3DB160.infowerks.com) on port 0/tcp 192.168.101.186 (ilas3db154.infowerks.com) on port 0/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 0/tcp 192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 0/tcp 192.168.101.111 (ilas1dc01.infowerks.com) on port 0/tcp

	192.168.101.187 (ilas2db10.infowerks.com) on port 0/tcp 192.168.100.185 (ILAS3WKS95.infowerks.com) on port 0/tcp 192.168.101.15 (ilas1fs02.infowerks.com) on port 0/tcp 192.168.101.160 (iwnv-w-wks-vminnick.infowerks.com) on port 0/tcp 192.168.101.184 (ilas3db140.infowerks.com) on port 0/tcp 192.168.100.18 (ilas3smtp01.infowerks.com) on port 0/tcp 192.168.101.122 (ILAS1DRN12.infowerks.com) on port 0/tcp 192.168.101.254 (ilas2fs05.infowerks.com) on port 0/tcp 192.168.101.198 (ILAS2IMG16.infowerks.com) on port 0/tcp 192.168.101.63 (imike.infowerks.com) on port 0/tcp 192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp 192.168.101.206 (ILAS4BCC2.infowerks.com) on port 0/tcp 192.168.100.54 (ILAS2WKS27.infowerks.com) on port 0/tcp 192.168.101.141 (ILAS1WKS09.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp 192.168.101.155 (ilas1iruntst1.infowerks.com) on port 0/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 0/tcp 192.168.100.100 (ILAS1WAGSWKS01.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.199.90 on port 0/tcp 192.168.101.175 (iSQL1.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp 192.168.101.221 (ilas1as09.infowerks.com) on port 0/tcp 192.168.101.185 (ilas3stor01.infowerks.com) on port 0/tcp 192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp

Additional Output

```
Description (Knowledge base entry)                                                    : Val
ue/Content
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
------------
Access to the registry possible (SMB/registry_access)                                 : TRU
E
Access via WMI possible (WMI/access_successful)                                       : FAL
SE
Architecture of the OS (SMB/Windows/Arch)                                             : x64
Build number of the OS (SMB/WindowsBuild)                                             : 190
45
Disable file search via WMI on Windows (win/lsc/disable_wmi_search)                   : FAL
SE
Disable the usage of win_cmd_exec for remote commands on Windows (win/lsc/disable_win_cmd_exec) : FAL
SE
Domain used for authenticated scans (kb_smb_domain())
------------ snipped ------------
```

BIOS and Hardware Information Detection (Windows SMB Login)

Severity	▮▯▯▯▯
Description	SMB login-based gathering of various BIOS and Hardware related information.
Affected Nodes	192.168.101.32 (ilas1fs01.infowerks.com) on port 0/tcp 192.168.100.171 (ILAS3WKS88.infowerks.com) on port 0/tcp 192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.101.14 (ilas1dc03.infowerks.com) on port 0/tcp 192.168.100.39 (ILAS1QA03.infowerks.com) on port 0/tcp 192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 0/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 0/tcp 192.168.101.112 (icage0dc02.infowerks.com) on port 0/tcp 192.168.101.232 (ILAS2IMG15.infowerks.com) on port 0/tcp

	192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.85 (ilas3wks04.infowerks.com) on port 0/tcp 192.168.100.200 (ilas3db05.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.101.66 (ilas1sql02.infowerks.com) on port 0/tcp 192.168.101.11 (ilas1bu02.infowerks.com) on port 0/tcp 192.168.100.159 (ILAS3WKS81.infowerks.com) on port 0/tcp 192.168.100.21 (ilas2ftp01.infowerks.com) on port 0/tcp 192.168.100.160 (ILAS3WKS82.infowerks.com) on port 0/tcp 192.168.101.192 (ILAS3DB160.infowerks.com) on port 0/tcp 192.168.101.186 (ilas3db154.infowerks.com) on port 0/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 0/tcp 192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 0/tcp 192.168.101.111 (ilas1dc01.infowerks.com) on port 0/tcp 192.168.101.187 (ilas2db10.infowerks.com) on port 0/tcp 192.168.100.185 (ILAS3WKS95.infowerks.com) on port 0/tcp 192.168.101.15 (ilas1fs02.infowerks.com) on port 0/tcp 192.168.101.184 (ilas3db140.infowerks.com) on port 0/tcp 192.168.101.122 (ILAS1DRN12.infowerks.com) on port 0/tcp 192.168.101.254 (ilas2fs05.infowerks.com) on port 0/tcp 192.168.101.198 (ILAS2IMG16.infowerks.com) on port 0/tcp 192.168.101.88 (ilas1sql04.infowerks.com) on port 0/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 0/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 0/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 0/tcp 192.168.100.54 (ILAS2WKS27.infowerks.com) on port 0/tcp 192.168.101.141 (ILAS1WKS09.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 0/tcp 192.168.101.175 (iSQL1.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp 192.168.101.221 (ilas1as09.infowerks.com) on port 0/tcp 192.168.101.185 (ilas3stor01.infowerks.com) on port 0/tcp 192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp

Additional Output	`BIOS version: 1.0.2`
	`BIOS Vendor: Dell Inc.`
	`Base Board version: A02`
	`Base Board Manufacturer: Dell Inc.`
	`Base Board Product Name: 0PJPW3`

Check for Windows 10 Cortana Search

Severity	▮▯▯▯▯
Description	Check for Windows 10 Cortana Search
Affected Nodes	192.168.100.171 (ILAS3WKS88.infowerks.com) on port 0/tcp 192.168.100.165 (ilas1win1003.infowerks.com) on port 0/tcp 192.168.101.14 (ilas1dc03.infowerks.com) on port 0/tcp 192.168.100.170 (ILAS3WKS87.infowerks.com) on port 0/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 0/tcp 192.168.101.112 (icage0dc02.infowerks.com) on port 0/tcp 192.168.101.159 (iwnv-w-wks-lvillegas.infowerks.com) on port 0/tcp 192.168.101.205 (ilas1as04.infowerks.com) on port 0/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 0/tcp 192.168.101.85 (ilas3wks04.infowerks.com) on port 0/tcp 192.168.100.200 (ilas3db05.infowerks.com) on port 0/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 0/tcp 192.168.100.159 (ILAS3WKS81.infowerks.com) on port 0/tcp 192.168.100.21 (ilas2ftp01.infowerks.com) on port 0/tcp 192.168.100.160 (ILAS3WKS82.infowerks.com) on port 0/tcp 192.168.100.69 (iwnv-w-wks-judd3.infowerks.com) on port 0/tcp 192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 0/tcp

	192.168.101.111 (ilas1dc01.infowerks.com) on port 0/tcp 192.168.101.187 (ilas2db10.infowerks.com) on port 0/tcp 192.168.100.185 (ILAS3WKS95.infowerks.com) on port 0/tcp 192.168.101.160 (iwnv-w-wks-vminnick.infowerks.com) on port 0/tcp 192.168.101.206 (ILAS4BCC2.infowerks.com) on port 0/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 0/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 0/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 0/tcp 192.168.101.194 (ilas1win1004.infowerks.com) on port 0/tcp
Additional Output	`Cortana Search is enabled.`

Compatibility Issues Affecting Signed Microsoft Binaries (2749655)

Severity	▂▃▅▆▇
Description	This host is missing an important security update according to Microsoft 2749655. Insight: Issue involving binaries that were signed with digital certificates generated by Microsoft without proper timestamp attributes. This issue is caused by a missing timestamp Enhanced Key Usage (EKU) extension during certificate generation and signing of Microsoft core components and software. Affected systems: - Microsoft Windows XP x32 Edition Service Pack 3 and prior - Microsoft Windows XP x64 Edition Service Pack 2 and prior - Microsoft Windows 7 x32/x64 Edition Service Pack 1 and prior - Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior - Microsoft Windows Vista x32/x64 Edition Service Pack 2 and prior - Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 and prior - Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2 and prior Impact: This could cause compatibility issues between affected binaries and Microsoft Windows and This issue could adversely impact the ability to properly install and uninstall affected Microsoft components and security updates.
Recommendation	Apply the patch from the referenced advisory.
References	Url: http://support.microsoft.com/kb/2749655 Url: http://support.microsoft.com/kb/2756872 Url: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2012/2749655
Affected Nodes	192.168.101.122 (ILAS1DRN12.infowerks.com) on port 0/tcp 192.168.101.175 (iSQL1.infowerks.com) on port 0/tcp

Cygwin Detection (Windows SMB Login)

Severity	▂▃▅▆▇
Description	Detects the installed version of Cygwin on Windows. The script logs in via smb, searches for Cygwin in the registry and gets the version.
Affected Nodes	192.168.100.160 (ILAS3WKS82.infowerks.com) on port 0/tcp

Additional Output	`Detected Cygwin`
	
	`Version:       Unknown`

```
Location:      C:\cygwin64
CPE:           cpe:/a:redhat:cygwin:x64
```

DCE/RPC and MSRPC Services Enumeration	
Severity	▂▃▄▆█
Description	Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. The actual reporting takes place in the VT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736) Impact: An attacker may use this fact to gain more knowledge about the remote host.
CVSS	0.0
Recommendation	Filter incoming traffic to this port.
Affected Nodes	192.168.100.18 (ilas3smtp01.infowerks.com) on port 135/tcp 192.168.100.21 (ilas2ftp01.infowerks.com) on port 135/tcp 192.168.100.39 (ILAS1QA03.infowerks.com) on port 135/tcp 192.168.100.54 (ILAS2WKS27.infowerks.com) on port 135/tcp 192.168.100.69 (iwnv-w-wks-judd3.infowerks.com) on port 135/tcp 192.168.100.159 (ILAS3WKS81.infowerks.com) on port 135/tcp 192.168.100.160 (ILAS3WKS82.infowerks.com) on port 135/tcp 192.168.100.164 (ilas1win1002.infowerks.com) on port 135/tcp 192.168.100.165 (ilas1win1003.infowerks.com) on port 135/tcp 192.168.100.170 (ILAS3WKS87.infowerks.com) on port 135/tcp 192.168.100.171 (ILAS3WKS88.infowerks.com) on port 135/tcp 192.168.100.184 (ILAS3WKS95a.infowerks.com) on port 135/tcp 192.168.100.185 (ILAS3WKS95.infowerks.com) on port 135/tcp 192.168.100.200 (ilas3db05.infowerks.com) on port 135/tcp 192.168.101.11 (ilas1bu02.infowerks.com) on port 135/tcp 192.168.101.14 (ilas1dc03.infowerks.com) on port 135/tcp 192.168.101.15 (ilas1fs02.infowerks.com) on port 135/tcp 192.168.101.32 (ilas1fs01.infowerks.com) on port 135/tcp 192.168.101.63 (imike.infowerks.com) on port 135/tcp 192.168.101.66 (ilas1sql02.infowerks.com) on port 135/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 135/tcp 192.168.101.83 (ilas1as23.infowerks.com) on port 135/tcp 192.168.101.84 (ilas3wks03.infowerks.com) on port 135/tcp 192.168.101.85 (ilas3wks04.infowerks.com) on port 135/tcp 192.168.101.88 (ilas1sql04.infowerks.com) on port 135/tcp 192.168.101.111 (ilas1dc01.infowerks.com) on port 135/tcp 192.168.101.112 (icage0dc02.infowerks.com) on port 135/tcp 192.168.101.122 (ILAS1DRN12.infowerks.com) on port 135/tcp 192.168.101.123 (ilas1drn13.infowerks.com) on port 135/tcp 192.168.101.125 (ilas1drn15.infowerks.com) on port 135/tcp 192.168.101.141 (ILAS1WKS09.infowerks.com) on port 135/tcp 192.168.101.154 (ilas3wks46.infowerks.com) on port 135/tcp 192.168.101.155 (ilas1iruntst1.infowerks.com) on port 135/tcp 192.168.101.159 (iwnv-w-wks-lvillegas.infowerks.com) on port 135/tcp 192.168.101.160 (iwnv-w-wks-vminnick.infowerks.com) on port 135/tcp 192.168.101.175 (iSQL1.infowerks.com) on port 135/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 135/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 135/tcp 192.168.101.183 (ILAS3IRUN04.infowerks.com) on port 135/tcp 192.168.101.184 (ilas3db140.infowerks.com) on port 135/tcp 192.168.101.185 (ilas3stor01.infowerks.com) on port 135/tcp 192.168.101.186 (ilas3db154.infowerks.com) on port 135/tcp 192.168.101.187 (ilas2db10.infowerks.com) on port 135/tcp 192.168.101.191 (ILAS2PG01.infowerks.com) on port 135/tcp 192.168.101.192 (ILAS3DB160.infowerks.com) on port 135/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 135/tcp

	192.168.101.194 (ilas1win1004.infowerks.com) on port 135/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 135/tcp 192.168.101.198 (ILAS2IMG16.infowerks.com) on port 135/tcp 192.168.101.205 (ilas1as04.infowerks.com) on port 135/tcp 192.168.101.206 (ILAS4BCC2.infowerks.com) on port 135/tcp 192.168.101.221 (ilas1as09.infowerks.com) on port 135/tcp 192.168.101.232 (ILAS2IMG15.infowerks.com) on port 135/tcp 192.168.101.254 (ilas2fs05.infowerks.com) on port 135/tcp 192.168.199.22 on port 135/tcp 192.168.199.40 on port 135/tcp 192.168.199.89 on port 135/tcp 192.168.199.90 on port 135/tcp
Additional Output	`A DCE endpoint resolution service seems to be running on this port.`

Dell DRAC / iDRAC Detection Consolidation

Severity	▮▯▯▯▯
Description	Consolidation of Dell Remote Access Controller (DRAC) / Integrated Remote Access Controller (iDRAC) detections.
References	Url: https://www.dell.com/en-us/lp/dt/open-manage-idrac
Affected Nodes	192.168.101.208 (ilas2db07.infowerks.com) on port 0/tcp

Additional Output	Detected Dell DRAC / iDRAC 8
	
	Version: 2.50.50.50
	Location: /
	CPE: cpe:/a:dell:idrac8:2.50.50.50
	
	Extra information:
	  Firmware build: 33
	
	Detection methods:
	
	- HTTP(s) on port 443/tcp
	  Concluded from version/product identification result:
	    fwVersionFull" :"2.50.50.50 (Build 33)
	    prodServerGen13G
	    .png hash: 8f8a11b24c183a5754b541ad9291545d
	  Concluded from version/product identification location:
	    https://ilas2db07.infowerks.com/login.html
	    https://ilas2db07.infowerks.com/session?aimGetProp=fwVersionFull
	    https://ilas2db07.infowerks.com/data?get=prodServerGen
	    https://ilas2db07.infowerks.com/images/Ttl_2_iDRAC8_Base_ML.png

Dell EMC OpenManage Server Administrator (OMSA) Detection (HTTP)

Severity	▮▯▯▯▯
Description	HTTP based detection of Dell EMC OpenManage Server Administrator (OMSA).
References	Url: https://www.dell.com/support/kbdoc/en-us/000132087/support-for-dell-emc-openmanage-server-administrator-omsa
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 1311/tcp 192.168.101.180 (ilas3db142.infowerks.com) on port 1311/tcp 192.168.101.181 (ILAS3DB161.infowerks.com) on port 1311/tcp 192.168.101.184 (ilas3db140.infowerks.com) on port 1311/tcp 192.168.101.186 (ilas3db154.infowerks.com) on port 1311/tcp 192.168.101.192 (ILAS3DB160.infowerks.com) on port 1311/tcp 192.168.101.193 (ILAS3DB162.infowerks.com) on port 1311/tcp 192.168.101.196 (ilas3db153.infowerks.com) on port 1311/tcp 192.168.101.254 (ilas2fs05.infowerks.com) on port 1311/tcp

Additional Output	Detected Dell EMC OpenManage Server Administrator (OMSA) Version: 8.5.0 Location: / CPE: cpe:/a:dell:emc_openmanage_server_administrator:8.5.0 Concluded from version/product identification result: Version 8.5.0 Concluded from version/product identification location: https://ilas3db142.infowerks.com:1311/Login?omacmd=getloginpage=Loginmanagedws=true https://ilas3db142.infowerks.com:1311/UDataArea?plugin=com.dell.oma.webplugins.AboutWebPlugin

'favicon.ico' Based Fingerprinting (HTTP)

Severity	▮▯▯▯▯
Description	HTTP based fingerprinting of web applications based on an exposed 'favicon.ico' file.
Affected Nodes	192.168.101.69 (ilas1as14.infowerks.com) on port 9084/tcp 192.168.101.221 (ilas1as09.infowerks.com) on port 9084/tcp 192.168.101.221 (ilas1as09.infowerks.com) on port 9087/tcp 192.168.101.69 (ilas1as14.infowerks.com) on port 9087/tcp
Additional Output	The following apps/services were identified: "jetty (5.1.14)" fingerprinted by the file: "http://ilas1as09.infowerks.com:9084/favicon.ico"