Date of Publication
July 2, 2025

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

June 2025

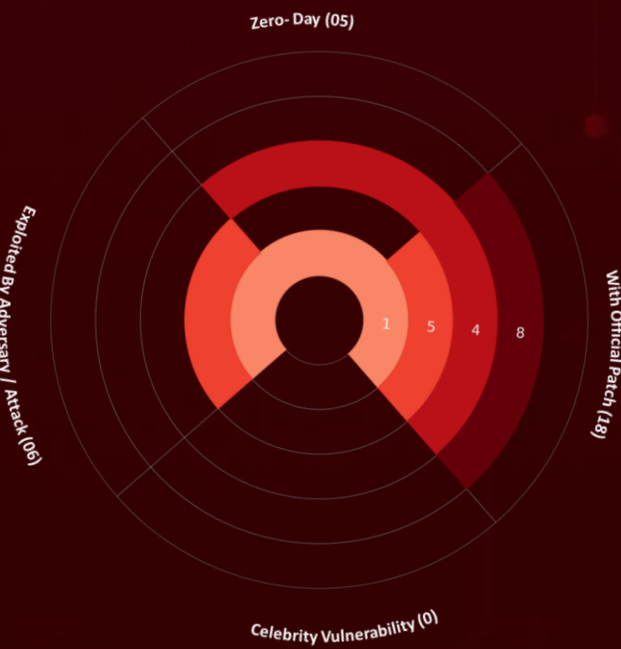
Table of Contents

Summary

The Known Exploited Vulnerability (KEV) catalog, maintained by CISA, is the authoritative source of vulnerabilities that have been exploited in the wild.

It is recommended that all organizations review and monitor the KEV catalog, prioritize remediation of listed vulnerabilities, and reduce the likelihood of compromise by threat actors. In June 2025, twenty vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, five are zero-day vulnerabilities; six have been exploited by known threat actors and employed in attacks.

20
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-6543	Citrix NetScaler ADC and Gateway Buffer Overflow Vulnerability	Citrix NetScaler ADC and Gateway	9.2	✗	✓	July 21, 2025
CVE-2019-6693	Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability	Fortinet FortiOS	6.5	✗	✓	July 16, 2025
CVE-2024-0769	D-Link DIR-859 Router Path Traversal Vulnerability	D-Link DIR-859 Router	9.8	✗	EOL	July 16, 2025
CVE-2024-54085	AMI MegaRAC SPx Authentication Bypass by Spoofing Vulnerability	AMI MegaRAC SPx	9.8	✗	✓	July 16, 2025
CVE-2023-0386	Linux Kernel Improper Ownership Management Vulnerability	Linux Kernel	7.8	✗	✓	July 8, 2025
CVE-2023-33538	TP-Link Multiple Routers Command Injection Vulnerability	TP-Link Multiple Routers	8.8	✗	EOL	July 7, 2025
CVE-2025-43200	Apple Multiple Products Unspecified Vulnerability	Apple Multiple Products	4.8	✗	✓	July 7, 2025
CVE-2025-33053	Microsoft Windows External Control of File Name or Path Vulnerability	Microsoft Windows	8.8	✓	✓	July 1, 2025
CVE-2025-24016	Wazuh Server Deserialization of Untrusted Data Vulnerability	Wazuh Server	9.9	✗	✓	July 1, 2025
CVE-2024-42009	RoundCube Webmail Cross-Site Scripting Vulnerability	RoundCube Webmail	9.3	✗	✓	June 30, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-32433	Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability	Erlang Erlang/OTP	10.0	✗	✓	June 30, 2025
CVE-2025-5419	Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	Google Chromium V8	8.8	✓	✓	June 26, 2025
CVE-2025-21479	Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability	Qualcomm Multiple Chipsets	8.6	✓	✓	June 24, 2025
CVE-2025-21480	Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability	Qualcomm Multiple Chipsets	8.6	✓	✓	June 24, 2025
CVE-2025-27038	Qualcomm Multiple Chipsets Use-After-Free Vulnerability	Qualcomm Multiple Chipsets	7.5	✓	✓	June 24, 2025
CVE-2021-32030	ASUS Routers Improper Authentication Vulnerability	ASUS Routers	9.8	✗	✓	June 23, 2025
CVE-2025-3935	ConnectWise ScreenConnect Improper Authentication Vulnerability	ConnectWise ScreenConnect	7.2	✗	✓	June 23, 2025
CVE-2025-35939	Craft CMS External Control of Assumed-Immutable Web Parameter Vulnerability	Craft CMS	5.3	✗	✓	June 23, 2025
CVE-2024-56145	Craft CMS Code Injection Vulnerability	Craft CMS	9.8	✗	✓	June 23, 2025
CVE-2023-39780	ASUS RT-AX55 Routers OS Command Injection Vulnerability	ASUS RT-AX55 Routers	8.8	✗	✓	June 23, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-6543	✗	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.46, 13.1 BEFORE 13.1-59.19 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1- 37.236-FIPS and NDcPP	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	-
Citrix NetScaler ADC and Gateway Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1190: Exploit Public-Facing Application; T1059: Command and Scripting; T1068: Exploitation for Privilege Escalation	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-6693	✗	FortiOS Version 6.2.0, 6.0.0 to 6.0.6, 5.6.10 and below	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	Akira, Snatch ransomware
Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-798	T1552.001: Credentials In Files	https://fortiguard.fortinet.com/psirt/FG-IR-19-007

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-0769	✗	D-Link DIR-859 Router	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dlink:dir-859_firmware:1.06:beta1:*:*:*:*:*:* cpe:2.3:h:dlink:dir-859:-:*:*:*:*:*:*:*	-
D-Link DIR-859 Router Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1068: Exploitation for Privilege Escalation	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-54085	✗	AMI MegaRAC SPx Version Prior to SPx_12.7+ and SPx_13.5	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:ami:megarac_sp-x:*:*:*:*:*:*:*:*	-
AMI MegaRAC SPx Authentication Bypass by Spoofing Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-290	T1068: Exploitation for Privilege Escalation	https://go.ami.com/hubfs/Security%20Advisories/2025/AMI-SA-2025003.pdf

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-0386	✗	Linux kernel versions prior to 6.2-rc6 (specifically 5.11 to <5.15.91; 5.16 to <6.1.9; 6.2:rc1 through 6.2:rc5)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*	-
Linux Kernel Improper Ownership Management Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	Cwe-282	T1068: Exploitation for Privilege Escalation	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4f11ada10d0a

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33538	✗	TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:tp-link:tl-wr940n_firmware:-:*:*:*:*:*:*:* cpe:2.3:o:tp-link:tl-wr841n_firmware:-:*:*:*:*:*:*:* cpe:2.3:o:tp-link:tl-wr740n_firmware:-:*:*:*:*:*:*:*	-
TP-Link Multiple Routers Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	EOL

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-43200</td><td>✕</td><td rowspan="2">watchOS Version Prior to 11.3.1, macOS Ventura Version Prior to 13.7.4, iOSVersion Prior to 15.8.4 and iPadOS Version Prior to 15.8.4, iOS Version Prior to 16.7.11 and iPadOS Version Prior to 16.7.11, iPadOS Version Prior to 17.7.5, visionOS Version Prior to 2.3.1, macOS Sequoia Version Prior to 15.3.1, iOS Version Prior to 18.3.1 and iPadOS Version Prior to 18.3.1</td><td>-</td></tr>
<tr><td>ZERO-DAY</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>✕</td><td>AFFECTED CPE</td><td>Graphite spyware</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="3">cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*</td><td></td></tr>
<tr><td>Apple Multiple Products Unspecified Vulnerability</td><td>✕</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>-</td><td>T1566.001: Spearphishing Attachment</td><td>https://support.apple.com/en-us/118575 , https://support.apple.com/en-us/108382 , https://support.apple.com/en-us/108926 , https://support.apple.com/en-us/118481</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-33053	✗	Windows: 10 - 11 24H2, Windows Server: 2008 - 2025	Stealth Falcon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Horus Agent, Horus Loader
Microsoft Windows External Control of File Name or Path Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1071.001: Web Protocols; T1071: Application Layer Protocol; T1071.002: File Transfer Protocols	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24016	✗	Wazuh Server version 4.4.0 to 4.9.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:wazuh:wazuh:*:*:*:*:*:*:*:*	Mirai, Resbot
Wazuh Server Deserialization of Untrusted Data Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059.006: Python; T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://github.com/wazuh/wazuh/releases/tag/v4.9.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-42009	✗	RoundCube Version Prior to 1.6.8 and 1.5.8	UNC1151
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
RoundCube Webmail Cross-Site Scripting Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1203: Exploitation for Client Execution	https://github.com/roundcube/roundcubemail/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32433	✗	All Erlang/OTP SSH servers running versions: OTP-27.3.2 and earlier OTP-26.2.5.10 and earlier OTP-25.3.2.19 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:erlang:otp:*:*:*:*:*:*:*:*	-
Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059: Command and Scripting Interpréter; T1059.004: Unix Shell; T1059.006: Python; T1133: External Remote Services; T1190: Exploit Public-Facing Application	https://github.com/erlang/otp/releases , https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-5419	✗ ZERO-DAY	Google Chrome prior to 137.0.7151.68 Microsoft Edge	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125 CWE-787	T1190: Exploit Public-Facing Application; T1566: Phishing; T1059: Command and Scripting Interpreter	https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.html , https://www.microsoft.com/en-us/edge/download?form=MA13FJ

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21479	✗ ZERO-DAY	Qualcomm Multiple Chipsets	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qualcomm:qualcomm:*:*:*:*:*:*:*:*	-
Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1068: Exploitation for Privilege Escalation; T1203: Exploitation for Client Execution	https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21480	✗	Qualcomm Multiple Chipsets	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qualcomm:qualcomm:*:*:*:*:*:*:*:*	-
Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1068: Exploitation for Privilege Escalation; T1203: Exploitation for Client Execution	https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-27038	✗	Qualcomm Multiple Chipsets	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qualcomm:qualcomm:*:*:*:*:*:*:*:*	-
Qualcomm Multiple Chipsets Use-After-Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1588.006: Vulnerabilities; T1203: Exploitation for Client Execution	https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-32030	✗	ASUS GT-AC2900 devices before 3.0.0.4.386.42643 and Lyra Mini before 3.0.0.4_384_46630	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:asus:lyra_mini_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:asus:gt-ac2900_firmware:*:*:*:*:*:*:*:*	-
ASUS Routers Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation	https://www.asus.com/supportonly/rog%20rapture%20gt-ac2900/helpdesk_bios/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-3935	✗	ScreenConnect versions 25.2.3 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*:*	-
ConnectWise ScreenConnect Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://www.connectwise.com/company/trust/security-bulletins/screenconnect-security-patch-2025.4

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-35939	✗	Craft CMS Version Prior to 5.7.5, Version Prior to 4.15.3	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:craftcms:craft_cms:*:*:*:*:*:*:*:*	-
Craft CMS External Control of Assumed-Immutable Web Parameter Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-472	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://github.com/craftcms/cms/releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-56145	✗	Craft CMS Version Prior to 3.9.14, Version Prior to 4.13.2, Version Prior to 5.5.2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:craftcms:craft_cms:*:*:*:*:*:*:*:*	-
Craft CMS Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://github.com/craftcms/cms/releases/

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-39780</td><td>  </td><td rowspan="2">ASUS RT-AX55 3.0.0.4.386.51598 devices</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:o:asus:rt-ax55_firmware:3.0.0.4.386.51598:*:*:*:*:*:*:*</td><td rowspan="2">AyySSHush botnet</td></tr>
<tr><td rowspan="3">ASUS RT-AX55 Routers OS Command Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-78</td><td>T1059: Command and Scripting Interpreter</td><td>https://www.asus.com/networking-iot-servers/wifi-6/all-series/rt-ax55/helpdesk_bios/?model2Name=RT-AX55</td></tr>
</table>

Recommendations

- To ensure the security of their systems and data, organizations should prioritize the vulnerabilities listed above and promptly apply patches to them before the due date provided.

- It is essential to comply with BINDING OPERATIONAL DIRECTIVE 22-01 provided by the Cyber security and Infrastructure Security Agency (CISA). This directive outlines the minimum cybersecurity standards that all federal agencies must follow to protect their organization from cybersecurity threats.

- The affected products listed in the report can help organizations identify assets that have been affected by KEVs, even without conducting a scan. These assets should be patched with priority to reduce the risk.

References

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Appendix

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

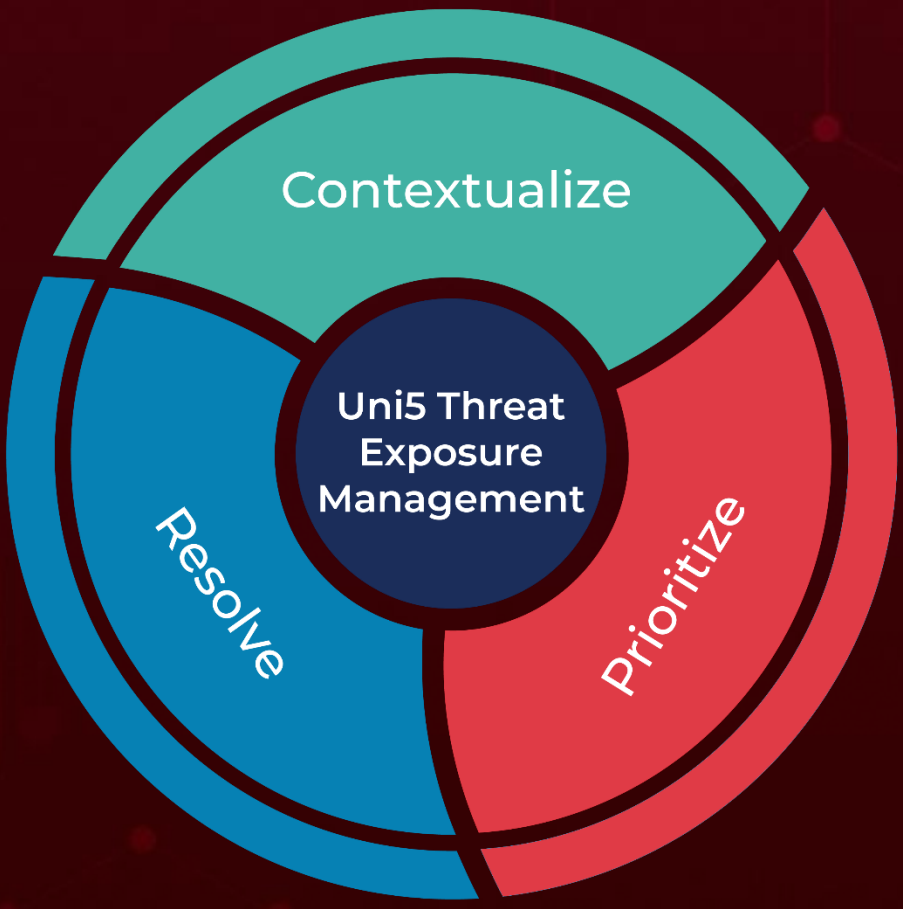
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

Due Date: The "Due Date" provided by CISA is a recommended deadline that organizations should use to prioritize the remediation of identified vulnerabilities in their systems, with the aim of enhancing their overall security posture.

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.



REPORT GENERATED ON

July 2, 2025 . 5:20 AM

More at www.hivepro.com