Date of Publication
August 4, 2025

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

July 2025

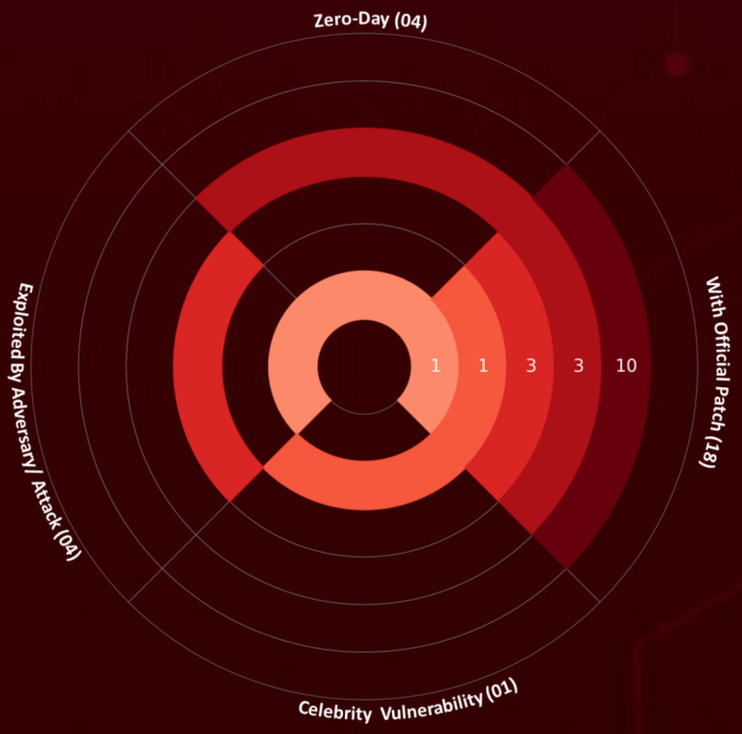
Table of Contents

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 July 2025, **twenty** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **four** are **zero-day** vulnerabilities; **four** 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-2023-2533	PaperCut NG/MF Cross-Site Request Forgery (CSRF) Vulnerability	PaperCut NG/MF	8.8	✗	✓	August 18, 2025
CVE-2025-20337	Cisco Identity Services Engine Injection Vulnerability	Cisco Identity Services Engine	10	✗	✓	August 18, 2025
CVE-2025-20281	Cisco Identity Services Engine Injection Vulnerability	Cisco Identity Services Engine	10	✗	✓	August 18, 2025
CVE-2025-2775	SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability	SysAid On-Prem	7.5	✗	✓	August 12, 2025
CVE-2025-2776	SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability	SysAid On-Prem	9.8	✗	✓	August 12, 2025
CVE-2025-6558	Google Chromium ANGLE and GPU Improper Input Validation Vulnerability	Google Chromium	8.8	✓	✓	August 12, 2025
CVE-2025-54309	CrushFTP Unprotected Alternate Channel Vulnerability	CrushFTP	9.8	✓	✓	August 12, 2025
CVE-2025-49704	Microsoft SharePoint Code Injection Vulnerability	Microsoft SharePoint	8.8	✗	✓	July 23, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2025-49706	Microsoft SharePoint Improper Authentication Vulnerability	Microsoft SharePoint	6.5	✗	✓	July 23, 2025
CVE-2025-53770	Microsoft SharePoint Deserialization of Untrusted Data Vulnerability	Microsoft SharePoint	9.8	✓	✓	July 21, 2025
CVE-2025-25257	Fortinet FortiWeb SQL Injection Vulnerability	Fortinet FortiWeb	9.8	✗	✓	August 8, 2025
CVE-2025-47812	Wing FTP Server Improper Neutralization of Null Byte or NUL Character Vulnerability	Wing FTP Server	10	✗	✓	August 4, 2025
CVE-2025-5777	Citrix NetScaler ADC and Gateway Out-of-Bounds Read Vulnerability	Citrix NetScaler ADC and Gateway	7.5	✗	✓	July 11, 2025
CVE-2019-9621	Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery (SSRF) Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	7.5	✗	✓	July 28, 2025
CVE-2019-5418	Rails Ruby on Rails Path Traversal Vulnerability	Ruby on Rails	7.5	✗	✓	July 28, 2025
CVE-2016-10033	PHPMailer Command Injection Vulnerability	PHPMailer	9.8	✗	✓	July 28, 2025
CVE-2014-3931	Multi-Router Looking Glass (MRLG) Buffer Overflow Vulnerability	Multi-Router Looking Glass (MRLG)	9.8	✗	✓	July 28, 2025
CVE-2025-6554	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8	8.1	✓	✓	July 23, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2025-48928	TeleMessage TM SGNL Exposure of Core Dump File to an Unauthorized Control Sphere Vulnerability	TeleMessage TM SGNL	4	⊗	⊗	July 22, 2025
CVE-2025-48927	TeleMessage TM SGNL Initialization of a Resource with an Insecure Default Vulnerability	TeleMessage TM SGNL	5.3	⊗	⊗	July 22, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-2533	❌	PaperCut NG and MF versions from 21.2.0 to 22.0.12	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*:*:*	-
PaperCut NG/MF Cross-Site Request Forgery (CSRF) Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-352	T1190: Exploit Public-Facing Application, T1059.007: JavaScript	https://www.papercut.com/kb/Main/SecurityBulletinJune2023

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-20337	❌	Cisco ISE and ISE-PIC releases 3.3 and 3.4	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:identity_services_engine:*:*:*:*:*:* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*:*:*:*:*:*	-
Cisco Identity Services Engine Injection Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-20281	⊗	Cisco ISE and ISE-PIC releases 3.3 and 3.4	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:identity_services_engine:*:*:*:*:*:* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*:*:*:*:*:*	-
Cisco Identity Services Engine Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-2775	⊗	SysAid On-Prem versions before 23.3.40 (inclusive)	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sysaid:sysaid:*:*:*:*:on-premises:*:*:*	-
SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1190: Exploit Public-Facing Application, T1001: Data Obfuscation	https://documentation.sysaid.com/docs/24-40-60

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-2776	✗	SysAid On-Prem versions before 23.3.40 (inclusive)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sysaid:sysaid:*:*:*:*:on-premises:*:*:*	-
SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1190: Exploit Public-Facing Application, T1001: Data Obfuscation	https://documentation.sysaid.com/docs/24-40-60

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-6558	✗	Google Chrome prior to 138.0.7204.157	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium ANGLE and GPU Improper Input Validation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1497: Virtualization/Sandbox Evasion, T1189: Drive-by Compromise	https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54309	✗	CrushFTP 10 before 10.8.5 and 11 before 11.3.4_23	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*:*:*	-
CrushFTP Unprotected Alternate Channel Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-420	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation; T1211: Exploitation for Defense Evasion	https://www.crushftp.com/download.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-49704	✗	Microsoft SharePoint Enterprise Server: 2016 - 2019	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*:*:*	Warlock ransomware, 4L4MD4R ransomware
Microsoft SharePoint Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49704

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-49706	☒	Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*:*:*	Warlock ransomware, 4L4MD4R ransomware
Microsoft SharePoint Improper Authentication Vulnerability	☒		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49706

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-53770	☒	Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, and Microsoft SharePoint Server Subscription Edition	Linen Typhoon, Violet Typhoon, Storm-2603
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_enterprise_server:-:*:*:*:*:*:*:*	Warlock ransomware, 4L4MD4R ransomware
Microsoft SharePoint Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-25257	✗	Fortinet FortiWeb versions: 7.6.0 - 7.6.3, 7.4.0 - 7.4.7, 7.2.0 - 7.2.10, 7.0.0 - 7.0.10	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*	-
Fortinet FortiWeb SQL Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application; T1059: Command and Scripting; T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-25-151

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-47812	✗	Wing FTP Server before 7.4.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:wftpserver:wing_ftp_server:*:*:*:*:*:*:*:*	-
Wing FTP Server Improper Neutralization of Null Byte or NUL Character Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-158	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1136: Create Account	https://www.wftpserver.com/download.htm

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-5777	CitrixBleed 2	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56, 13.1 BEFORE 13.1-58.32 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS	-
	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 Out-of-Bounds Read Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1190: Exploit Public-Facing Application, T1059: Command and Scripting, T1068: Exploitation for Privilege Escalation	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-9621	✗	Zimbra Collaboration Suite before 8.6 patch 13, 8.7.x before 8.7.11 patch 10, and 8.8.x before 8.8.10 patch 7 or 8.8.x before 8.8.11	Earth Lusca
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:*	SprySOCKS Backdoor
Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery (SSRF) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-918, CWE-807	T1190: Exploit Public-Facing Application, T1046: Network Service Discovery	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.7.11/P11, https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.9/P10, https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.10/P8, https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.11/P4

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-5418	✗	Rails versions <5.2.2.1, <5.1.6.2, <5.0.7.2, <4.2.11.1 and v3	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:rubyonrails:rails:*:*:*:*:*:*:*:*	-
Rails Ruby on Rails Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application	https://rubyonrails.org/category/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-10033	✗	PHPMailer before 5.2.18	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:phpmailer_project:phpmailer:*:*:*:*:*:*:*:*	-
PHPMailer Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77, CWE-88	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/PHPMailer/PHPMailer/releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-3931	✗	MRLG (aka Multi-Router Looking Glass) before 5.5.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:multi-router_looking_glass_project:multi-router_looking_glass:*:*:*:*:*:*:*:*	-
Multi-Router Looking Glass (MRLG) Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://mrlg.op-sec.us/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-6554	✗	Google Chrome prior to 138.0.7204.96	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium V8 Type Confusion Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1189: Drive-by Compromise, T1068: Exploitation for Privilege Escalation	https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48928	✗	TeleMessage TM SGNL	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:smarsh:telemessage:-:*:*:*:*:*:*:*:*	-
TeleMessage TM SGNL Exposure of Core Dump File to an Unauthorized Control Sphere Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-528	T1119: Automated Collection, T1552.001: Credentials In Files	✗

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-48927</td><td>☒</td><td rowspan="2">TeleMessage TM SGNL</td><td rowspan="2">-</td></tr>
<tr><td><b>ZERO-DAY</b></td></tr>
<tr><td>☒</td><td><b>AFFECTED CPE</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td></tr>
<tr><td><b>NAME</b></td><td><b>BAS ATTACKS</b></td><td rowspan="2">cpe:2.3:a:smarsh:telemessage:-:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">TeleMessage TM SGNL Initialization of a Resource with an Insecure Default Vulnerability</td><td>☒</td></tr>
<tr><td><b>CWE ID</b></td><td><b>ASSOCIATED TTPs</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>CWE-1188</td><td>T1495: Firmware Corruption, T1211: Exploitation for Defense Evasion</td><td>☒</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.

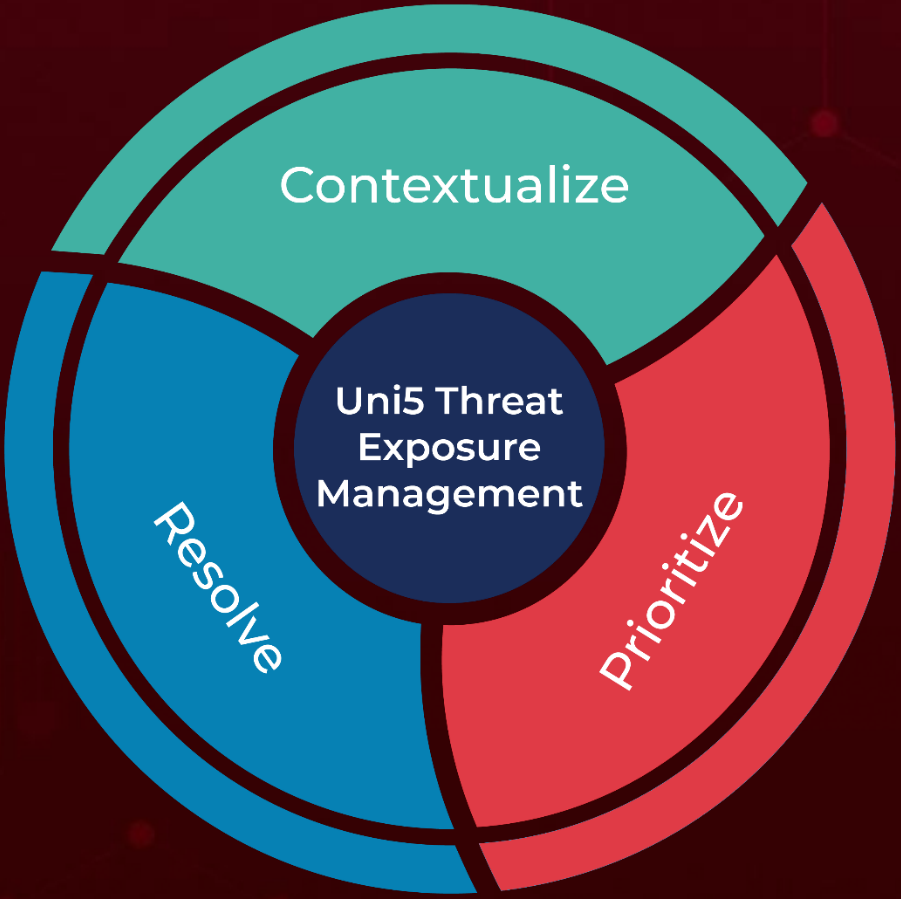
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

August 4, 2025 • 10:30 PM

More at www.hivepro.com