Date of Publication
November 4, 2025

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

October 2025

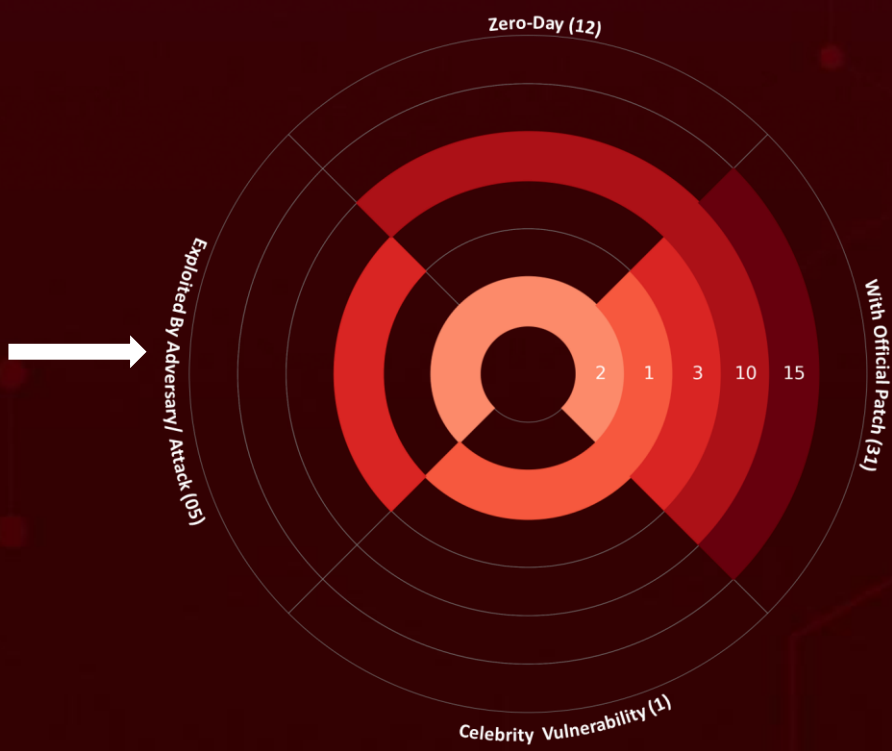
Table of Contents

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 October 2025, **31** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **twelve** are **zero-day** vulnerabilities; **five** have been **exploited** by known threat actors and employed in attacks.

31
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-41244	Broadcom VMware Aria Operations and VMware Tools Privilege Defined with Unsafe Actions Vulnerability	Broadcom VMware Aria Operations and VMware Tools	7.8	✓	✓	November 20, 2025
CVE-2025-24893	XWiki Platform Eval Injection Vulnerability	XWiki Platform	9.8	✗	✓	November 20, 2025
CVE-2025-6204	Dassault Systèmes DELMIA Apriso Code Injection Vulnerability	Dassault Systèmes DELMIA Apriso	8	✗	✓	November 18, 2025
CVE-2025-6205	Dassault Systèmes DELMIA Apriso Missing Authorization Vulnerability	Dassault Systèmes DELMIA Apriso	9.1	✗	✓	November 18, 2025
CVE-2025-54236	Adobe Commerce and Magento Improper Input Validation Vulnerability	Adobe Commerce and Magento	9.1	✗	✓	November 14, 2025
CVE-2025-59287	Microsoft Windows Server Update Service (WSUS) Deserialization of Untrusted Data Vulnerability	Microsoft Windows	9.8	✗	✓	November 14, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2025-61932	Motex LANSCOPE Endpoint Manager Improper Verification of Source of a Communication Channel Vulnerability	Motex LANSCOPE Endpoint Manager	9.8	✓	✓	November 12, 2025
CVE-2022-48503	Apple Multiple Products Unspecified Vulnerability	Apple Multiple Products	8.8	✗	✓	November 10, 2025
CVE-2025-2746	Kentico Xperience CMS Authentication Bypass Using an Alternate Path or Channel Vulnerability	Kentico Xperience CMS	9.8	✗	✓	November 10, 2025
CVE-2025-2747	Kentico Xperience CMS Authentication Bypass Using an Alternate Path or Channel Vulnerability	Kentico Xperience CMS	9.8	✗	✓	November 10, 2025
CVE-2025-33073	Microsoft Windows SMB Client Improper Access Control Vulnerability	Microsoft Windows	8.8	✗	✓	November 10, 2025
CVE-2025-61884	Oracle E-Business Suite Server-Side Request Forgery (SSRF) Vulnerability	Oracle E-Business Suite	7.5	✗	✓	November 10, 2025
CVE-2025-54253	Adobe Experience Manager Forms Code Execution Vulnerability	Adobe Experience Manager (AEM) Forms	10	✗	✓	November 5, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2025-47827	IGEL OS Use of a Key Past its Expiration Date Vulnerability	IGEL OS	4.6	✓	✓	November 4, 2025
CVE-2025-24990	Microsoft Windows Untrusted Pointer Dereference Vulnerability	Microsoft Windows	7.8	✓	✓	November 4, 2025
CVE-2025-59230	Microsoft Windows Improper Access Control Vulnerability	Microsoft Windows	7.8	✓	✓	November 4, 2025
CVE-2016-7836	SKYSEA Client View Improper Authentication Vulnerability	SKYSEA Client View	9.8	✗	✓	November 4, 2025
CVE-2021-43798	Grafana Path Traversal Vulnerability	Grafana Labs Grafana	7.5	✓	✓	October 30, 2025
CVE-2025-27915	Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	5.4	✓	✓	October 28, 2025
CVE-2021-22555	Linux Kernel Heap Out-of-Bounds Write Vulnerability	Linux Kernel	7.8	✗	✓	October 27, 2025
CVE-2010-3962	Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability	Microsoft Internet Explorer	8.1	✓	✓	October 27, 2025
CVE-2021-43226	Microsoft Windows Privilege Escalation Vulnerability	Microsoft Windows	7.8	✗	✓	October 27, 2025
CVE-2013-3918	Microsoft Windows Out-of-Bounds Write Vulnerability	Microsoft Windows	8.8	✗	✓	October 27, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2011-3402	Microsoft Windows Remote Code Execution Vulnerability	Microsoft Windows	8.8	✓	✓	October 27, 2025
CVE-2010-3765	Mozilla Multiple Products Remote Code Execution Vulnerability	Mozilla Multiple Products	9.8	✓	✓	October 27, 2025
CVE-2025-61882	Oracle E-Business Suite Unspecified Vulnerability	Oracle E-Business Suite	9.8	✓	✓	October 27, 2025
CVE-2014-6278	GNU Bash OS Command Injection Vulnerability	GNU Bash	8.8	✗	✓	October 23, 2025
CVE-2017-1000353	Jenkins Remote Code Execution Vulnerability	Jenkins	9.8	✗	✓	October 23, 2025
CVE-2015-7755	Juniper ScreenOS Improper Authentication Vulnerability	Juniper ScreenOS	9.8	✗	✓	October 23, 2025
CVE-2025-21043	Samsung Mobile Devices Out-of-Bounds Write Vulnerability	Samsung Mobile Devices	9.8	✓	✓	October 23, 2025
CVE-2025-4008	Smartbedded Meteobridge Command Injection Vulnerability	Smartbedded Meteobridge	8.8	✗	✓	October 23, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-41244		VMware Cloud Foundation and VMware vSphere Foundation: VMware Cloud Foundation Operations Version Prior to 9.0.1.0, VMware Cloud Foundation and VMware vSphere Foundation: VMware Tools Version Prior to 3.0.5.0, Prior to 13.0.5, Prior to 12.5.4, VMware Cloud Foundation: VMware Aria Operations Version 5.x, 4.x, VMware Aria Operations Version Prior to 8.18.5	UNC5174 (aka Uteus)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:vmware_cloud_foundation_operations:*:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vmware_tools:*:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vmware_aria_operations:*:*:*:*:*:*:*:*:*	-
Broadcom VMware Aria Operations and VMware Tools Privilege Defined with Unsafe Actions Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-267	T1068: Exploitation for Privilege Escalation, T1036.005: Masquerading: Match Legitimate Resource Name or Location	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-24893</td><td>✗</td><td rowspan="2">xwiki 5.3-milestone-2 - 15.10.11, 16.0.0-rc-1 - 16.4.1</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:a:xwiki:xwiki:*:*:*:*:*:*:*:*</td><td rowspan="2">tcrond</td></tr>
<tr><td rowspan="3">XWiki Platform Eval Injection Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94, CWE-95</td><td>T1059: Command and Scripting Interpreter</td><td>https://github.com/xwiki/xwiki-platform/commit/67021db9b8ed26c2236a653269302a86bf01ef40</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-6204	✗	DELMIA Apriso from Release 2020 through Release 2025	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:3ds:delmia_apriso:*:*:*:*:*:*:*:*	-
Dassault Systèmes DELMIA Apriso Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6204

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-6205	✗	DELMIA Apriso from Release 2020 through Release 2025	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:3ds:delmia_apriso:*:*:*:*:*:*:*:*	-
Dassault Systèmes DELMIA Apriso Missing Authorization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1562: Impair Defenses, T1078: Valid Accounts	https://www.3ds.com/trust-center/security/security-advisories/cve-2025-6205

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-54236</td><td>SessionReaper</td><td rowspan="2">Adobe Commerce Versions: 2.4.9- alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6- p12, 2.4.5-p14, 2.4.4-p15 and earlier
Adobe Commerce B2B Versions: 1.5.3-alpha2, 1.5.2-p2, 1.4.2-p7, 1.3.4-p14, 1.3.3-p15 and earlier
Magento Open Source Versions: 2.4.9-alpha2, 2.4.8-p2, 2.4.7 p7, 2.4.6-p12, 2.4.5-p14 and earlier</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:a:adobe:commerce:-:*:*:*:*:*:*:*
cpe:2.3:a:adobe:commerce_b2b:-:*:*:*:*:*:*:*
cpe:2.3:a:adobe:magento:-:*:*:open_source:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Adobe Commerce and Magento Improper Input Validation Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-20</td><td>T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1539: Steal Web Session Cookie</td><td>https://helpx.adobe.com/security/products/magento/apsb25-88.html</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-59287	✗	Windows Server 2012, 2016, 2019, 2022, 2025	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows Server Update Service (WSUS) Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-61932	✗	LANSCOPE Endpoint Manager On-Premise Version 9.4.7.1 and earlier Client Program (MR) Detection Agent (DA)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:motex:lanscope_endpoint_manager:*:*:*:*:on-premise:*:*:*	-
Motex LANSCOPE Endpoint Manager Improper Verification of Source of a Communication Channel Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-940	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1210: Exploitation of Remote Services; T1068: Exploitation for Privilege Escalation; T1203: Exploitation for Client Execution	https://www.motex.co.jp/news/notice/2025/release251020/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-48503		Apple affected iPadOS versions before 15.6., Apple affected iPhone OS versions before 15.6., Apple affected macOS versions from and including 12.0.0 up to but not including 12.5., Apple affected Safari versions before 15.6., Apple affected tvOS versions before 15.6., Apple affected watchOS versions before 8.7.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*	-
Apple Multiple Products Unspecified Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-129	T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/102879, https://support.apple.com/en-us/102893, https://support.apple.com/en-us/102878, https://support.apple.com/en-us/102891, https://support.apple.com/en-us/102892

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-2746	✗	Kentico Xperience through 13.0.172.	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:kentico:xperience:*:*:*:*:*:*:*:*	-
Kentico Xperience CMS Authentication Bypass Using an Alternate Path or Channel Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1211: Exploitation for Defense Evasion	https://devnet.kentico.com/download/hotfixes

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTORS
CVE-2025-2747	✗	Kentico Xperience through 13.0.178.	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:kentico:xperience:*:*:*:*:*:*:*:*	-
Kentico Xperience CMS Authentication Bypass Using an Alternate Path or Channel Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1211: Exploitation for Defense Evasion	https://devnet.kentico.com/download/hotfixes

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-33073	✗	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows SMB Client Improper Access Control Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1068: Exploitation for Privilege Escalation, T1548: Abuse Elevation Control Mechanism	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTORS
CVE-2025-61884	✗	Oracle E-Business Suite 12.2.3-12.2.14.	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:configurator:*:*:*:*:*:*:*:*	-
Oracle E-Business Suite Server-Side Request Forgery (SSRF) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-444, CWE-501, CWE-287, CWE-22, CWE-918, CWE-93	T1090: Proxy, T1135: Network Share Discovery, T1005: Data from Local System, T1133: External Remote Service	https://www.oracle.com/security-alerts/alert-cve-2025-61884.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54253	✗	Adobe Experience Manager (AEM) Forms on JEE version 6.5.23.0 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:experience_manager:*:*:*:*:-:*:*:*	-
Adobe Experience Manager Forms Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1068: Exploitation for Privilege Escalation, T1190 : Exploit Public-Facing Application	https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTORS
CVE-2025-47827	✗	Windows Server 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2, IGEL OS before 11	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_serve:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:igel:igel_os:*:*:*:*:*:*:*:*	-
IGEL OS Use of a Key Past its Expiration Date Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-347	T1068: Exploitation for Privilege Escalation, T1547 : Boot or Logon Autostart Execution	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-47827

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24990	✗	Windows Server 2008, 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_serve:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
Microsoft Windows Untrusted Pointer Dereference Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-822	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-24990

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTORS
CVE-2025-59230	✗	Windows Server 2008, 2012, 2016, 2019, 2022, 2025; Windows 10 - 11 25H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_serve:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
Microsoft Windows Improper Access Control Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59230

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-7836	✗	SKYSEA Client View Ver.11.221.03 and earlier	BRONZE BUTLER
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:skygroup:skysea_client_view:*:*:*:*:*:*:*:*	-
SKYSEA Client View Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-287	T1078: Valid Accounts, T1556: Modify Authentication Process	https://www.skyseaclientview.net/news/161221/ https://www.skygroup.jp/security-info/news/170308.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-43798	✗	Grafana versions 8.0.0-beta1 through 8.3.0	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:grafana:grafana:*:*:*:*:*:*:*:*	-
Grafana Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22	T1190: Exploit Public-Facing Application, T1083: File and Directory Discovery	https://github.com/grafana/grafana/security/advisories/GHSA-8pjx-jj86-j47p https://grafana.com/blog/2021/12/08/an-update-on-0day-cve-2021-43798-grafana-directory-traversal/

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-27915</td><td>✗</td><td rowspan="2">Zimbra Collaboration (ZCS) 9.0, 10.0, and 10.1</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:a:zimbra:collaboration:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-79</td><td>T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter</td><td>https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.13, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.5, https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P44</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22555	✗	Linux since v2.6.19-rc1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Heap Out-of-Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1499: Endpoint Denial of Service, T1068: Exploitation for Privilege Escalation	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/net/netfilter/x_tables.c?id=9fa492cdc160cd27ce1046cb36f47d3b2b1efa21, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/net/netfilter/x_tables.c?id=b29c457a6511435960115c0f548c4360d5f4801d

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2010-3962	✗	Microsoft Internet Explorer 6, 7, and 8	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:internet_explorer:-:*:*:*:*:*:*:*	-
Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1105: Ingress Tool Transfer	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-090

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2021-43226</td><td>✗</td><td rowspan="2">Windows: 7 - 11 21H2 10.0.22000.194, Windows Server: 2008 - 2019 2004</td><td rowspan="2">Andariel</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:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft Windows Privilege Escalation Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-264</td><td>T1068: Exploitation for Privilege Escalation</td><td>https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-43226</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2013-3918</td><td>  </td><td rowspan="2">Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*
cpe:2.3:o:microsoft:windows_serve:-:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft Windows Out-of-Bounds Write Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-119</td><td>T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter</td><td>https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-090</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2011-3402		Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_serve:-:*:*:*:*:*:*:*	-
Microsoft Windows Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1059: Command and Scripting Interpreter	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-087

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2010-3765		Mozilla Firefox 3.5.x through 3.5.14 and 3.6.x through 3.6.11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:*	-
Mozilla Multiple Products Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1059: Command and Scripting Interpreter	https://www.mozilla.org/en-US/security/advisories/mfsa2010-73/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-61882	✗ ZERO-DAY	Oracle E-Business Suite versions 12.2.3-12.2.14	Scattered Spider, ShinyHunters, and LAPSUS$
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:concurrent_processing:*:*:*:*:*:*:*:*	Cl0p Ransomware
Oracle E-Business Suite Unspecified Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22 CWE-444	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://www.oracle.com/security-alerts/alert-cve-2025-61882.html, https://www.oracle.com/security-alerts/, https://support.oracle.com/rs?type=doc&id=3106344.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-6278	✗ ZERO-DAY	GNU Bash through 4.3 bash43-026	-
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gnu:bash:-:*:*:*:*:*:*:*	-
GNU Bash OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://ftp.gnu.org/gnu/bash/bash-4.3-patches/bash43-027

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-1000353	✗	Jenkins versions 2.56 and earlier as well as 2.46.1 LTS and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:jenkins:jenkins:*:*:*:*:-:*:*:*	-
Jenkins Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://www.jenkins.io/security/advisory/2017-04-26/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-7755	✗	Juniper ScreenOS: 6.3.0r17 - 6.3.0r20	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:juniper:screenos:-:*:*:*:*:*:*:*	-
Juniper ScreenOS Improper Authentication Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1078: Valid Accounts, T1556: Modify Authentication Process	https://supportportal.juniper.net/s/article/2015-12-Out-of-Cycle-Security-Bulletin-ScreenOS-Multiple-Security-issues-with-ScreenOS-CVE-2015-7755-CVE-2015-7756

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21043	✗	Samsung Mobile Firmware: SMR-DEC-2015 - SMR-APR-2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:samsung:android:-:*:*:*:*:*:*:*	-
Samsung Mobile Devices Out-of-Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1203: Exploitation for Client Execution, T1204.002: User Execution: Malicious Link, T1059: Command and Scripting Interpreter	https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=09

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4008	✗	MeteoBridge: before 6.2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:smartbedded:meteobridge:*:*:*:*:*:*:*:*	-
Smartbedded Meteobridge Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306, CWE-77	T1059: Command and Scripting Interpreter	https://forum.meteohub.de/viewtopic.php?t=18687

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.

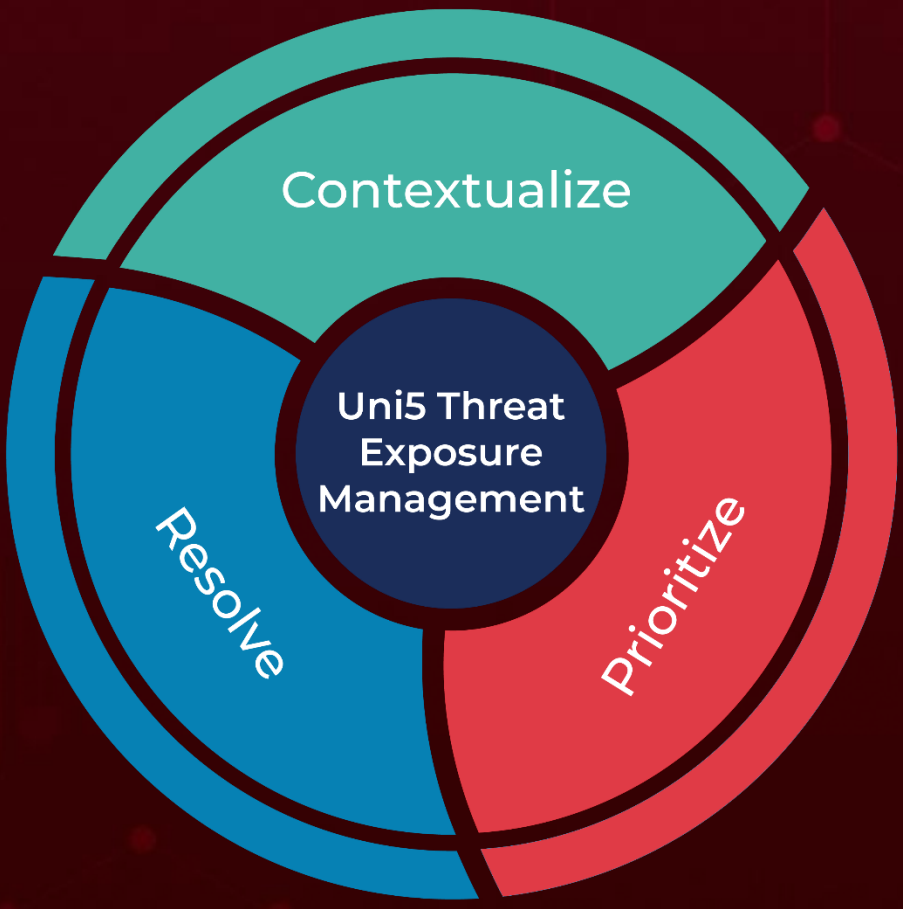
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

November 4, 2025 • 10:30 PM

More at www.hivepro.com