Date of Publication
March 4, 2025

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

February 2025

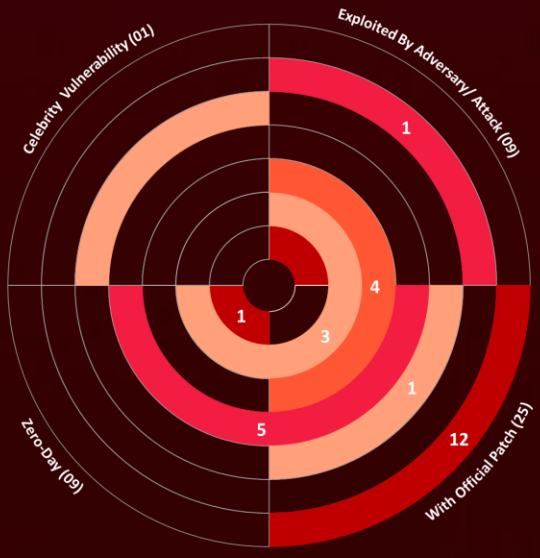
Table of Contents

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

27
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-34192	Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	9	✗	✓	March 18, 2025
CVE-2024-49035	Microsoft Partner Center Improper Access Control Vulnerability	Microsoft Partner Center	8.7	✗	✓	March 18, 2025
CVE-2024-20953	Oracle Agile Product Lifecycle Management (PLM) Deserialization Vulnerability	Oracle Agile Product Lifecycle Management (PLM)	8.8	✗	✓	March 17, 2025
CVE-2017-3066	Adobe ColdFusion Deserialization Vulnerability	Adobe ColdFusion	9.8	✗	✓	March 17, 2025
CVE-2025-24989	Microsoft Power Pages Improper Access Control Vulnerability	Microsoft Power Pages	8.2	✗	✓	March 14, 2025
CVE-2025-0111	Palo Alto Networks PAN-OS File Read Vulnerability	Palo Alto Networks PAN-OS	6.5	✗	✓	March 13, 2025
CVE-2025-23209	Craft CMS Code Injection Vulnerability	Craft CMS Craft CMS	8	✓	✓	March 13, 2025
CVE-2025-0108	Palo Alto Networks PAN-OS Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS	9.1	✗	✓	March 11, 2025
CVE-2024-53704	SonicWall SonicOS SSLVPN Improper Authentication Vulnerability	SonicWall SonicOS	9.8	✗	✓	March 11, 2025
CVE-2024-57727	SimpleHelp Path Traversal Vulnerability	SimpleHelp SimpleHelp	7.5	✗	✓	March 6, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-24200	Apple iOS and iPadOS Incorrect Authorization Vulnerability	Apple iOS and iPadOS	6.1	✓	✓	March 5, 2025
CVE-2024-41710	Mitel SIP Phones Argument Injection Vulnerability	Mitel SIP Phones	7.2	✗	✓	March 5, 2025
CVE-2024-40891	Zyxel DSL CPE OS Command Injection Vulnerability	Zyxel DSL CPE Devices	8.8	✓	✗	March 4, 2025
CVE-2024-40890	Zyxel DSL CPE OS Command Injection Vulnerability	Zyxel DSL CPE Devices	8.8	✗	✗	March 4, 2025
CVE-2025-21418	Microsoft Windows Ancillary Function Driver for WinSock Heap-Based Buffer Overflow Vulnerability	Microsoft Windows	7.8	✓	✓	March 4, 2025
CVE-2025-21391	Microsoft Windows Storage Link Following Vulnerability	Microsoft Windows	7.1	✓	✓	March 4, 2025
CVE-2025-0994	Trimble Cityworks Deserialization Vulnerability	Trimble Cityworks	8.8	✓	✓	February 28, 2025
CVE-2020-15069	Sophos XG Firewall Buffer Overflow Vulnerability	Sophos XG Firewall	9.8	✓	✓	February 27, 2025
CVE-2020-29574	CyberoamOS (CROS) SQL Injection Vulnerability	Sophos CyberoamOS	9.8	✓	✓	February 27, 2025
CVE-2024-21413	Microsoft Outlook Improper Input Validation Vulnerability	Microsoft Office Outlook	9.8	✗	✓	February 27, 2025
CVE-2022-23748	Dante Discovery Process Control Vulnerability	Audinate Dante Discovery	7.8	✗	✓	February 27, 2025
CVE-2025-0411	7-Zip Mark of the Web Bypass Vulnerability	7-Zip 7-Zip	7	✓	✓	February 27, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-53104	Linux Kernel Out-of-Bounds Write Vulnerability	Linux Kernel	7.8	✗	✓	February 26, 2025
CVE-2018-19410	Paessler PRTG Network Monitor Local File Inclusion Vulnerability	Paessler PRTG Network Monitor	9.8	✗	✓	February 25, 2025
CVE-2018-9276	Paessler PRTG Network Monitor OS Command Injection Vulnerability	Paessler PRTG Network Monitor	7.2	✗	✓	February 25, 2025
CVE-2024-29059	Microsoft .NET Framework Information Disclosure Vulnerability	Microsoft .NET Framework	7.5	✗	✓	February 25, 2025
CVE-2024-45195	Apache OFBiz Forced Browsing Vulnerability	Apache OFBiz	7.5	✗	✓	February 25, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34192	✗	Zimbra Collaboration Suite (ZCS) v.8.8.15	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:zimbra:collaboration:8.8.15:-:*:*:*:*:*:*	-
Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-79	T1189: Drive-by Compromise, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-49035	✗	Microsoft Partner Center	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:partner_center:-:*:*:*:*:*:*:*	-
Microsoft Partner Center Improper Access Control Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1190: Exploit Public-Facing Application T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49035

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20953	✗	Oracle Agile PLM version 9.3.6	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:agile_product_lifecycle_management:*:*:*:*:*:*:*:*	-
Oracle Agile Product Lifecycle Management (PLM) Deserialization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.oracle.com/security-alerts/cpujan2024.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-3066	✗	Adobe ColdFusion 2016 Update 3 and earlier, ColdFusion 11 update 11 and earlier, ColdFusion 10 Update 22 and earlier	Rocke
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:coldfusion:-:*:*:*:*:*:*:*	Sysrv Botnet
Adobe ColdFusion Deserialization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://helpx.adobe.com/security/products/coldfusion/apsb17-14.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24989	✗	Microsoft Power Pages	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:power_pages:-:*:*:*:*:*:*:*	-
Microsoft Power Pages Improper Access Control Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24989

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-0111	✗	PAN-OS 10.1.0 to 10.1.14 PAN-OS 10.2.0 to 10.2.13 PAN-OS 11.1.0 to 11.1.6 PAN-OS 11.2.0 to 11.2.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS File Read Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1190: Exploit Public-Facing Application, T1005: Data from Local System, T1068: Exploitation for Privilege Escalation	https://security.paloaltonetworks.com/CVE-2025-0111

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-23209</td><td>  </td><td rowspan="2">Craft CMS Versions:
>= 4.0.0-RC1 and < 4.13.8,
>= 5.0.0-RC1 and < 5.5.8</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:craftcms:craft_cms:-:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Craft CMS Code Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94</td><td>T1059: Command and Scripting Interpreter</td><td>https://github.com/craftcms/cms/security/advisories/GHSA-x684-96hh-833x</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-0108	✗	PAN-OS 10.1 versions earlier than 10.1.14-h9 PAN-OS 10.2 versions earlier than 10.2.13-h3 PAN-OS 11.1 versions earlier than 11.1.6-h1 PAN-OS 11.2 versions earlier than 11.2.4-h4 PAN-OS 11.0 (EOL)	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-306	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://security.paloaltonetworks.com/CVE-2025-0108

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53704	✗	SonicWALL Gen7 NSv Version Prior to 7.0.1-5165, SonicWALL Gen7 Firewalls Version Prior to 7.1.3-7015, SonicWALL TZ80 Version Prior to 8.0.0-8037	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:o:sonicwall:sonicos:*:*:*:*:*:*:*:*	-
SonicWall SonicOS SSLVPN Authentication Bypass Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-287	T1556: Modify Authentication Process, T1133: External Remote Services, T1068: Exploitation for Privilege Escalation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-57727	✗	SimpleHelp remote support software v5.5.7 and before	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*:*:*	Silver
SimpleHelp Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1133: External Remote Services, T1190: Exploit Public-Facing Application	https://simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24200	✗	Apple iPadOS Version before 17.7.5, Apple iOS and iPadOS Version before 18.3.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apple:ipados:*:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*:*	-
Apple iOS and iPadOS Incorrect Authorization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1068: Exploitation for Privilege Escalation	https://support.apple.com/en-us/118575

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-41710	✗	Mitel SIP Phones	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:mitel:sip_firmware:*:*:*:*:*:*:*:*	Aquabotv3
Mitel SIP Phones Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-88	T1059: Command and Scripting Interpreter	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-24-0019

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-40891	✗	Zyxel CPE Series	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:zyxel:cpe:*:*:*:*:*:*	Mirai
Zyxel CPE Telnet Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	No Patch

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-40890	✗	Zyxel CPE Series	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:zyxel:cpe:*:*:*:*:*:*	Mirai
Zyxel CPE Telnet Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	No Patch

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21418	✗	Windows Server 2008, 2012, 2016, 2019, 2022, 2025 Windows 10, 11	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21418

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21391	✗	Windows 10, 11 Windows Server 2016, 2019, 2022, 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Windows Storage Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-59	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-21391

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-0994	✗	Trimble Cityworks versions prior to 15.8.9 and Cityworks with office companion versions prior to 23.10	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:trimble:cityworks:*:*:*:*:*:*:*:*	-
Trimble Cityworks Deserialization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	Trimble Cityworks version 15.8.9 and Cityworks with office companion version 23.10

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-15069		Sophos XG Firewall 17.x through v17.5 MR12	TStark
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:sophos:xg_firewall_firmware:*:*:*:*:*:*:*:*	-
Sophos XG Firewall Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1505.003: Server Software Component: Web Shell	https://www.sophos.com/en-us/security-advisories/sophos-sa-20200625-xg-user-portal-rce

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-29574		Cyberoam OS Versions upto 2020-12-04	Chinese state-sponsored groups
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:sophos:cyberoamos:*:*:*:*:*:*:*:*	-
CyberoamOS (CROS) SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1136.001 Create Account: Local Account	https://www.sophos.com/en-us/security-advisories/sophos-sa-20201210-cyberoam-webadmin-sqli

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21413	MonikerLink ZERO-DAY	Microsoft Office: 2016 - 2019 Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	-
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	-
Microsoft Outlook Improper Input Validation Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-20	T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-23748	✗ ZERO-DAY	mDNSResponder.exe v1.3.1 and earlier Dante Application Library for Windows v1.2.0 and earlier	ToddyCat
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:audinate:dante_application_library:*:*:*:*:*:*:*:*	CurKeep, CurLu, CurLog
Dante Discovery Process Control Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-114	T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1059.003: Windows Command Shell	https://www.audinate.com/learning/faqs/audinate-response-to-dante-discovery-mdnsresponder-exe-security-issue-cve-2022-23748

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-0411	✗	7-Zip Version Prior to 24.09	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:7-zip:7-zip:*:*:*:*:*:*:*:*	SmokeLoader
7-Zip Mark-of-the-Web Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1059: Command and Scripting Interpreter; T1553.005: Mark-of-the-Web Bypass	https://www.7-zip.org/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53104	✗	Linux Kernel	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Out-of-Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1204: User Execution T1068: Exploitation for Privilege Escalation	https://web.git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=1ee9d9122801eb688783acd07791f2906b87cb4f

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-19410	✗	PRTG Network Monitor before 18.2.40.1683	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:paessler:prtg_network_monitor:*:*:*:*:*:*:*:*	-
Paessler PRTG Network Monitor Local File Inclusion Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://www.paessler.com/prtg/history/prtg-18#18.2.41.1652

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-9276	✗	PRTG Network Monitor before 18.2.39	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:paessler:prtg_network_monitor:*:*:*:*:*:*:*:*	-
Paessler PRTG Network Monitor OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://www.paessler.com/prtg/history/prtg-18#18.2.39

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29059	✗	Microsoft .NET Framework	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:.net_framework:3.5:-:*:*:*:*:*:*	-
Microsoft .NET Framework Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-209	T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29059

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-45195	✗	Apache OFBiz: Version Prior to 18.12.16	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*:*:*	-
Apache OFBiz Forced Browsing Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-425	T1190: Exploit Public-Facing Application, T1204: User Execution, T1068: Exploitation for Privilege Escalation	https://ofbiz.apache.org/download.html

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.

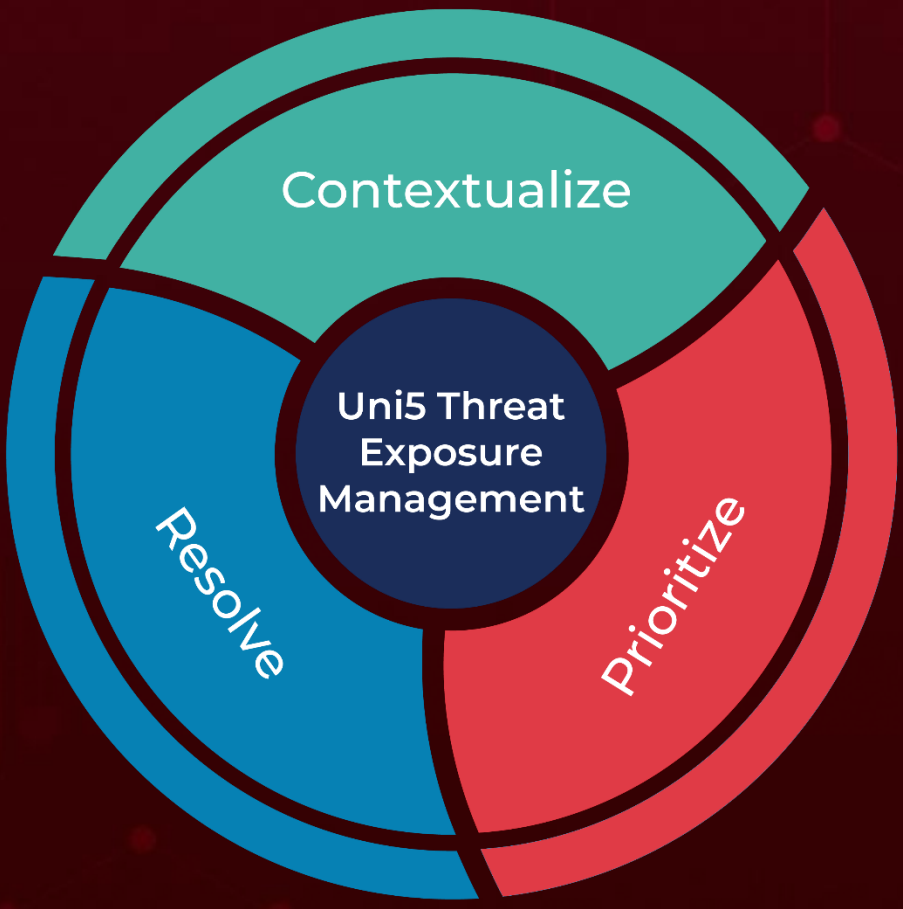
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

March 4, 2025 • 5:30 AM

More at www.hivepro.com