Date of Publication
May 07, 2026

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

April 2026

Table of Contents

Summary 03

CVEs List 04

CVEs Details 10

Recommendations 38

References 39

Appendix 39

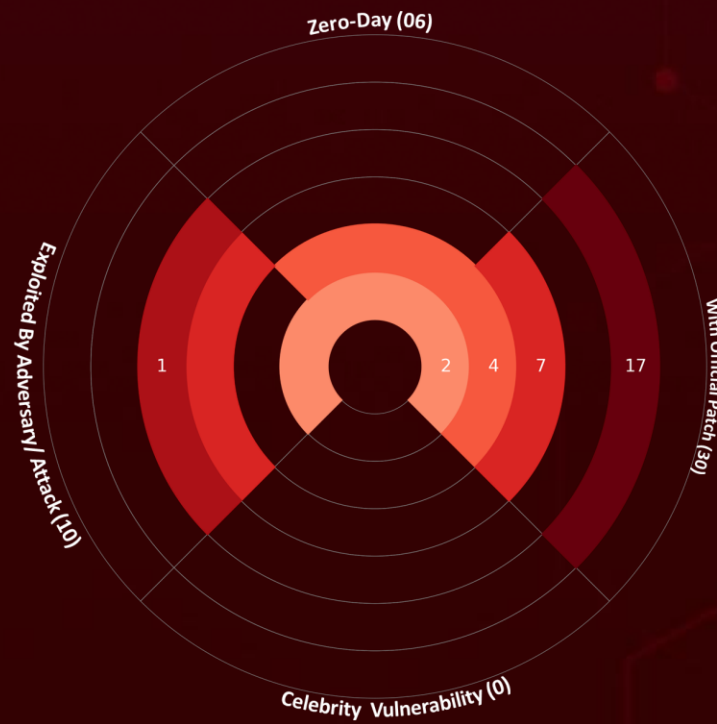
What Next? 40

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 **April 2026**, **31** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **6** are **zero-day** vulnerabilities; **10** have been **exploited** by a threat actor and employed in attacks.

31
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-41940	WebPros cPanel & WHM and WP2 (WordPress Squared) Missing Authentication for Critical Function Vulnerability	WebPros cPanel & WHM and WP2 (WordPress Squared)	9.8	✓	✓	May 03, 2026
CVE-2024-1708	ConnectWise ScreenConnect Path Traversal Vulnerability	ConnectWise ScreenConnect	8.4	✗	✓	May 12, 2026
CVE-2026-32202	Microsoft Windows Protection Mechanism Failure Vulnerability	Microsoft Windows	4.3	✗	✓	May 12, 2026
CVE-2025-29635	D-Link DIR-823X Command Injection Vulnerability	D-Link DIR-823X	7.2	✗	✗	May 08, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-7399	Samsung MagicINFO 9 Server Path Traversal Vulnerability	Samsung MagicINFO 9 Server	9.8	✗	✓	May 08, 2026
CVE-2024-57728	SimpleHelp Path Traversal Vulnerability	SimpleHelp	7.2	✗	✓	May 08, 2026
CVE-2024-57726	SimpleHelp Missing Authorization Vulnerability	SimpleHelp	9.9	✗	✓	May 08, 2026
CVE-2026-39987	Marimo Remote Code Execution Vulnerability	Marimo	9.8	✗	✓	May 07, 2026
CVE-2026-33825	Microsoft Defender Insufficient Granularity of Access Control Vulnerability	Microsoft Defender	7.8	✗	✓	May 06, 2026
CVE-2026-20122	Cisco Catalyst SD-WAN Manager Incorrect Use of Privileged APIs Vulnerability	Cisco Catalyst SD-WAN Manger	5.4	✗	✓	April 23, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-20133	Cisco Catalyst SD-WAN Manager Exposure of Sensitive Information to an Unauthorized Actor Vulnerability	Cisco Catalyst SD-WAN Manager	7.5	✗	✓	April 23, 2026
CVE-2025-2749	Kentico Xperience Path Traversal Vulnerability	Kentico Xperience	7.2	✗	✓	May 04, 2026
CVE-2023-27351	PaperCut NG/MF Improper Authentication Vulnerability	PaperCut NG/MF	7.5	✗	✓	May 04, 2026
CVE-2025-48700	Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	6.1	✗	✓	April 23, 2026
CVE-2026-20128	Cisco Catalyst SD-WAN Manager Storing Passwords in a Recoverable Format Vulnerability	Cisco Catalyst SD-WAN Manager	7.5	✗	✓	April 23, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-32975	Quest KACE Systems Management Appliance (SMA) Improper Authentication Vulnerability	Quest KACE Systems Management Appliance (SMA)	10			May 04, 2026
CVE-2024-27199	JetBrains TeamCity Relative Path Traversal Vulnerability	JetBrains TeamCity	7.3			May 04, 2026
CVE-2026-34197	Apache ActiveMQ Improper Input Validation Vulnerability	Apache ActiveMQ	8.8			April 30, 2026
CVE-2009-0238	Microsoft Office Remote Code Execution	Microsoft Office	8.8			April 28, 2026
CVE-2026-32201	Microsoft SharePoint Server Improper Input Validation Vulnerability	Microsoft SharePoint Server	6.5			April 28, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2012-1854	Microsoft Visual Basic for Applications Insecure Library Loading Vulnerability	Microsoft Visual Basic for Applications (VBA)	7.8			April 27, 2026
CVE-2025-60710	Microsoft Windows Link Following Vulnerability	Microsoft Windows	7.8			April 27, 2026
CVE-2023-21529	Microsoft Exchange Server Deserialization of Untrusted Data Vulnerability	Microsoft Exchange Server	8.8			April 27, 2026
CVE-2023-36424	Microsoft Windows Out-of-Bounds Read Vulnerability	Microsoft Windows	7.8			April 27, 2026
CVE-2020-9715	Adobe Acrobat Use-After-Free Vulnerability	Adobe Acrobat	7.8			April 27, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-21643	Fortinet FortiClient EMS SQL Injection Vulnerability	Fortinet FortiClient EMS	9.8	✗	✓	April 16, 2026
CVE-2026-34621	Adobe Acrobat and Reader Prototype Pollution Vulnerability	Adobe Acrobat and Reader	8.6	✗	✓	April 27, 2026
CVE-2026-1340	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	9.8	✓	✓	April 11, 2026
CVE-2026-35616	Fortinet FortiClient EMS Improper Access Control Vulnerability	Fortinet FortiClient EMS	9.8	✓	✓	April 09, 2026
CVE-2026-3502	TrueConf Client Download of Code Without Integrity Check Vulnerability	TrueConf Client	7.8	✓	✓	April 16, 2026
CVE-2026-5281	Google Dawn Use-After-Free Vulnerability	Google Dawn	8.8	✓	✓	April 15, 2026

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-41940		cPanel and WHM versions after v11.40, and v136.1.7 of WP Squared	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cpanel:cpanel:*:*:*:*:*:*:*:*	Sorry ransomware
WebPros cPanel & WHM and WP2 (WordPress Squared) Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059:Command and Scripting Interpreter, T1068:Exploitation for Privilege Escalation	https://support.cpanel.net/hc/en-us/articles/40073787579671-Security-CVE-2026-41940-cPanel-WHM-WP2-Security-Update-04-28-2026

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-1708</td><td>  </td><td rowspan="2">ScreenConnect 23.9.7 and prior</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:connectwise:screenconnect:*:*:*:*:*:*:*:*</td><td rowspan="2">LockBit ransomware, BlackBasta Ransomware, Bl00dy Ransomware, Blackcat Ransomware, XWORM, and AsyncRAT</td></tr>
<tr><td>ConnectWise ScreenConnect Path Traversal Vulnerability</td><td>  </td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-22</td><td>T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities</td><td>https://screenconnect.connectwise.com/download</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-32202	✗	Windows Server 2012, 2025, Windows 11, 10	APT28
	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 Protection Mechanism Failure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1562: Impair Defenses, T1211: Exploitation for Defense Evasion, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32202

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-29635</td><td>✗</td><td rowspan="2">D-Link DIR-823X 240126 and 240802</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:h:dlink:dir-823x:-:*:*:*:*:*:*:*:*; cpe:2.3:o:dlink:dir-823x_firmware:*:*:*:*:*:*:*:*</td><td rowspan="2">Mirai Botnet</td></tr>
<tr><td rowspan="2">D-Link DIR-823X Command Injection Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-77</td><td>T1059: Command and scripting interpreter</td><td>EOL - https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10469</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-2024-7399</td><td>  </td><td rowspan="2">Samsung MagicINFO 9 Server Versions prior to 21.1050</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:samsung:magicinfo_9_server:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Samsung MagicINFO 9 Server Path Traversal Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-22, CWE-434</td><td>T1068: Exploitation for Privilege Escalation</td><td>https://eu.community.samsung.com/t5/samsung-solutions/update-magicinfo-server-v9-update-procedure-for-v7-v8-and-v9/ta-p/11374265</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-2024-57728</td><td>  </td><td rowspan="2">SimpleHelp remote support software v5.5.7 and before</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><th>NAME</th><th>BAS ATTACKS</th><td rowspan="2">cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*:*:*</td><td rowspan="2">DragonForce Ransomware</td></tr>
<tr><td rowspan="3">SimpleHelp Path Traversal Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-22</td><td>T1566: Phishing, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://guides.simple-help.com/kb---security-vulnerabilities-01-2025#security-vulnerabilities-in-simplehelp-5-5-7-and-earlier</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-57726		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:*:*:*:*:*:*:*:*	DragonForce Ransomware
SimpleHelp Missing Authorization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://guides.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-2026-39987	✗	Marimo versions before 0.23.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:marimo-team:marimo:*:*:*:*:*:python:*:*	-
Marimo Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059.006 Command and Scripting Interpreter: Python	https://github.com/marimo-team/marimo/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-2026-33825</td><td>  </td><td rowspan="2">Microsoft Defender</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:microsoft:microsoft_defender:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft Defender Insufficient Granularity of Access Control Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-1220</td><td>T1068: Exploitation for Privilege Escalation, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1006: Direct Volume Access</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20122	✗	Cisco Catalyst SD-WAN Manager (Before 20.9.8.2 / 20.12.6.1 / 20.15.4.2 / 20.18.2.1)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Manager Incorrect Use of Privileged APIs Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-648	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20133	✗	Cisco Catalyst SD-WAN Manager (Before 20.9.8.2 / 20.12.6.1 / 20.15.4.2 / 20.18.2.1)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Manager Exposure of Sensitive Information to an Unauthorized Actor Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-2749	✗	Kentico Xperience through 13.0.178.	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:kentico:xperience:*:*:*:*:*:*:*:*	-
Kentico Xperience Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22, CWE-434	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	https://devnet.kentico.com/download/hotfixes

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-27351</td><td>✕</td><td rowspan="2">PaperCut NG: before 22.0.9, PaperCut MF: before 22.0.9</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:papercut:papercut_mf:*:*:*:*:*:*:*:*</td><td rowspan="2">Bl00dy Ransomware
Clop Ransomware
LockBit Ransomware
DiceLoader
TrueBot
and Cobalt Strike Beacons</td></tr>
<tr><td rowspan="3">PaperCut NG/MF Improper Authentication Vulnerability</td><td>✕</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-287</td><td>T1059:Command and Scripting Interpreter, T1068:Exploitation for Privilege Escalation</td><td>https://www.papercut.com/kb/Main/PO-1216-and-PO-1219</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-2025-48700</td><td>  </td><td rowspan="2">Zimbra Collaboration (ZCS) 8.8.15 and 9.0 and 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:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:*</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 LINK</td></tr>
<tr><td>CWE-79</td><td>T1059: Command and Scripting Interpreter, T1204: User Execution, T1539: Steal Web Session Cookie</td><td>https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20128		Cisco Catalyst SD-WAN Manager (Before 20.18)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Manager Storing Passwords in a Recoverable Format Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-257	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-32975</td><td>  </td><td rowspan="2">Quest KACE Systems Management Appliance (SMA) 13.0.x before 13.0.385, 13.1.x before 13.1.81, 13.2.x before 13.2.183, 14.0.x before 14.0.341 (Patch 5), and 14.1.x before 14.1.101 (Patch 4)</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:quest:kace_systems_management_appliance:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Quest KACE Systems Management Appliance (SMA) Improper Authentication Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-287</td><td>T1059:Command and Scripting Interpreter, T1068:Exploitation for Privilege Escalation</td><td>https://support.quest.com/kb/4379499/quest-response-to-kace-sma-vulnerabilities-cve-2025-32975-cve-2025-32976-cve-2025-32977-cve-2025-32978</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27199		TeamCity On-Premises	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*:*:*	Jasmin ransomware, XMRig, SparkRAT backdoor
JetBrains TeamCity Relative Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-23	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	https://www.jetbrains.com/teamcity/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-34197		Apache ActiveMQ Broker (Before 5.19.4, 6.0.0 Before 6.2.3), Apache ActiveMQ (Before 5.19.4, 6.0.0 before 6.2.3)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:activemq:*:*:*:*:*:*:*:*; cpe:2.3:a:apache:activemq_broker:*:*:*:*:*:*:*:*	-
Apache ActiveMQ Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20, CWE-94	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://activemq.apache.org/download.html

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="4">CVE-2009-0238</td><td>  </td><td rowspan="2">Microsoft Office Excel 2000 SP3, 2002 SP3, 2003 SP3, and 2007 SP1; Excel Viewer 2003 Gold and SP3; Excel Viewer; Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1; and Excel in Microsoft Office 2004 and 2008 for Mac</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:microsoft:office_excel_viewer:*:*:*:*:*:*:*:*;
cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*:*;
cpe:2.3:a:microsoft:excel:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft Office Remote Code Execution</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-009</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-2026-32201</td><td>  </td><td rowspan="2">Microsoft Office SharePoint Server</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:microsoft:sharepoint_server:*:*:*:*:subscription:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft SharePoint Server 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>T1190 Exploit Public-Facing Application, T1036 Masquerading, T1656 Impersonation</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201</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-2012-1854</td><td>  </td><td rowspan="2">VBE6.dll in Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; Microsoft Visual Basic for Applications (VBA); and Summit Microsoft Visual Basic for Applications SDK</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*:*; cpe:2.3:a:microsoft:visual_basic_for_applications:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Microsoft Visual Basic for Applications Insecure Library Loading Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-426</td><td>T1574: Hijack Execution Flow, T1059: Command and Scripting Interpreter, T1574.001: DLL Search Order Hijacking, T1574.001: DLL Side-Loading</td><td>https://learn.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-046</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-2025-60710</td><td>  </td><td rowspan="2">Windows Server 2025, Windows 11 Version</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:microsoft:windows_11_24h2:*:*:*:*:*:*:*:*; cpe:2.3:o:microsoft:windows_server_2025:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft Windows Link Following Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-59</td><td>T1574: Hijack Execution Flow, T1068: Exploitation for Privilege Escalation, T1222: File and Directory Permissions Modification</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-60710</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-2023-21529</td><td>  </td><td rowspan="2">Microsoft Exchange Server 2016, 2013, 2019</td><td rowspan="2">Storm-1175</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:microsoft:exchange_server:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft Exchange Server Deserialization of Untrusted Data Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-502</td><td>502T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36424		Windows Server 2012, 2008, 2016, 2022, 2019; Windows 10, 11 Version	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_10_1507:*:*:*:*:*:*:*:*; cpe:2.3:o:microsoft:windows_server_2008:*:*:*:*:*:*:*:*	-
Microsoft Windows Out-of-Bounds Read Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1068: Exploitation for Privilege Escalation, T1212: Exploitation for Credential Access, T1005: Data from Local System	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-9715		Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:acrobat_dc:*:*:*:*:*:*:*:*; cpe:2.3:a:adobe:acrobat_reader_dc:*:*:*:*:*:*:*:*:*	-
Adobe Acrobat Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1203: Exploitation for Client Execution, T1204: User Execution, T1204.002: Malicious File	https://helpx.adobe.com/security/products/acrobat/apsb20-48.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21643		Fortinet FortiClient EMS 7.4.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:forticlientems:*:*:*:*:*:*:*:*:*	-
Fortinet FortiClient EMS SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and scripting interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-25-1142

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="4">CVE-2026-34621</td><td>  </td><td rowspan="2">Adobe Acrobat DC (26.001.21367 and earlier), Adobe Acrobat Reader DC (26.001.21367 and earlier), Adobe Acrobat 2024 (24.001.30356 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:acrobat_dc:*:*:*:*:continuous:*:*:*; cpe:2.3:a:adobe:acrobat_reader_dc:*:*:*:*:continuous:*:*:*; cpe:2.3:a:adobe:acrobat:*:*:*:*:classic:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Adobe Acrobat and Reader Prototype Pollution Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-1321</td><td>T1203: Exploitation for Client Execution, T1059.007 Command and Scripting Interpreter: JavaScript</td><td>https://helpx.adobe.com/security/products/acrobat/apsb26-43.html</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-1340		Ivanti EPMM Versions 12.5.0.0 and prior, 12.6.0.0 and prior, 12.7.0.0 and prior, 12.5.1.0 and prior, 12.6.1.0 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.0.0:*:*:*:*:*:*:*; cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.0.0:*:*:*:*:*:*:*; cpe:2.3:a:ivanti:endpoint_manager_mobile:12.7.0.0:*:*:*:*:*:*:*; cpe:2.3:a:ivanti:endpoint_manager_mobile:12.5.1.0:*:*:*:*:*:*:*; cpe:2.3:a:ivanti:endpoint_manager_mobile:12.6.1.0:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-35616		Fortinet FortiClient EMS version 7.4.5 through 7.4.6	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:forticlientems:*:*:*:*:*:*:*:*:*	-
Fortinet FortiClient EMS Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1562.001: Disable or Modify Tools, T1059: Command and scripting interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-26-099

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-3502		TrueConf Client for Windows (versions 8.1.0 through 8.5.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:trueconf:trueconf_client:*:*:*:*:*:windows:*:*	Havoc
TrueConf Client Download of Code Without Integrity Check Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-494	T1195.002: Supply Chain Compromise, T1072: Software Deployment Tools	https://trueconf.com/downloads/windows.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-5281		Microsoft Edge (Chromium-based), Google Chrome	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*; cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Dawn Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189 Drive-by Compromise, T1203 Exploitation for Client Execution, T1068 Exploitation for Privilege Escalation	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

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 Demo of **HivePro**.

REPORT GENERATED ON

May 07, 2026 • 03:00 AM

More at www.hivepro.com