Date of Publication
July 02, 2026

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

June 2026

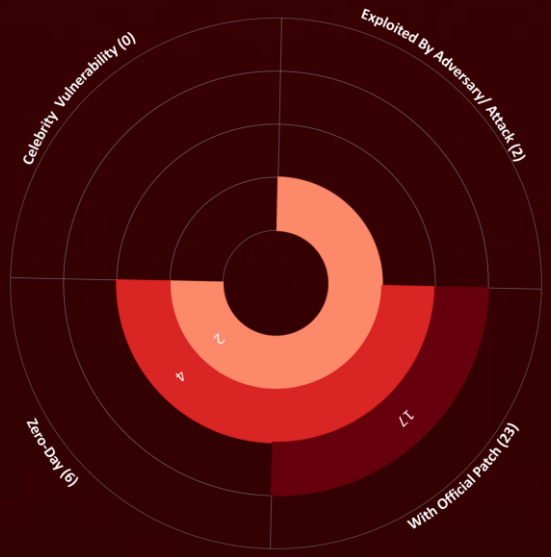
Table of Contents

Summary

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

It is recommended that all organizations review and monitor the KEV catalog, prioritize remediation of listed vulnerabilities, and reduce the likelihood of compromise by threat actors. In **June 2026**, **23** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **6** are **zero-day** vulnerabilities, **2** have been **exploited** by named threat actors and employed in attacks.

23
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-48558	SimpleHelp Authentication Bypass Vulnerability	SimpleHelp	10	✗	✓	July 02, 2026
CVE-2026-12569	PTC Windchill and FlexPLM Improper Input Validation Vulnerability	PTC Windchill and FlexPLM	9.8	✗	✓	June 28, 2026
CVE-2026-20230	Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability	Cisco Unified Communications Manager	8.6	✗	✓	June 28, 2026
CVE-2025-67038	Lantronix EDS5000 Code Injection Vulnerability	Lantronix EDS5000	9.8	✗	✓	June 26, 2026
CVE-2026-34910	Ubiquiti UniFi OS Improper Input Validation Vulnerability	Ubiquiti UniFi OS	10	✗	✓	June 26, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-34909	Ubiquiti UniFi OS Path Traversal Vulnerability	Ubiquiti UniFi OS	10	✗	✓	June 26, 2026
CVE-2026-34908	Ubiquiti UniFi OS Improper Access Control Vulnerability	Ubiquiti UniFi OS	10	✗	✓	June 26, 2026
CVE-2026-20253	Splunk Enterprise Missing Authentication for Critical Function Vulnerability	Splunk Enterprise	9.8	✗	✓	June 21, 2026
CVE-2026-48907	Widget Factory Joomla Content Editor Improper Access Control Vulnerability	Widget Factory Joomla Content Editor	9.8	✗	✓	June 19, 2026
CVE-2026-54420	LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability	LiteSpeed cPanel Plugin	8.5	✗	✓	June 18, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-20262	Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability	Cisco Catalyst SD-WAN Manager	6.5	✓	✓	June 29, 2026
CVE-2026-35273	Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability	Oracle PeopleSoft Enterprise PeopleTools	9.8	✓	✓	June 15, 2026
CVE-2026-10520	Ivanti Sentry OS Command Injection Vulnerability	Ivanti Sentry	10	✗	✓	June 14, 2026
CVE-2026-11645	Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	Google Chromium V8	8.8	✓	✓	June 23, 2026
CVE-2026-7473	Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability	Arista Extensible Operating System	5.8	✗	✓	June 23, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-20245	Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability	Cisco Catalyst SD-WAN Manager	7.8	✓	✓	June 23, 2026
CVE-2026-42271	BerriAI LiteLLM Command Injection Vulnerability	BerriAI LiteLLM	8.8	✗	✓	June 22, 2026
CVE-2026-50751	Check Point Security Gateway Improper Authentication Vulnerability	Check Point Security Gateway	9.3	✓	✓	June 11, 2026
CVE-2026-28318	SolarWinds Serv-U Uncontrolled Resource Consumption Vulnerability	SolarWinds Serv-U	7.5	✗	✓	June 19, 2026
CVE-2026-45247	Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data Vulnerability	Mirasvit Mirasvit Full Page Cache Warmer	9.8	✗	✓	June 06, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2022-0492	Linux Kernel Improper Authentication Vulnerability	Linux Kernel	7.8			June 05, 2026
CVE-2025-48595	Android Framework Integer Overflow Vulnerability	Android Framework	8.4			June 05, 2026
CVE-2024-21182	Oracle WebLogic Server Unspecified Vulnerability	Oracle WebLogic Server	7.5			June 04, 2026

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-48558		SimpleHelp versions 5.5.15 and prior and 6.0 pre-release versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:simple-help:simplehelp:*:*:*:*:*:*:*:*	TaskWeaver Djinn Stealer
SimpleHelp Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-347	T1190: Exploit Public-Facing Application, T1606: Forge Web Credentials, T1136: Create Account	https://simple-help.com/security/simplehelp-security-update-2026-05

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-12569</td><td>✗</td><td rowspan="2">PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030</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:ptc:windchill_pdmlink:*:*:*:*:*:*:*:*:*
cpe:2.3:a:ptc:flexplm:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">PTC Windchill and FlexPLM 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, T1505.003: Server Software Component: Web Shell, T1059: Command and Scripting Interpreter</td><td>https://www.ptc.com/en/support/article/CS473270</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-2026-20230</td><td>  </td><td rowspan="2">Cisco Unified Communications Manager (Unified CM) and Unified CM SME, release 14 (before 14SU6) and release 15 (before 15SU5 / COP1), with WebDialer enabled</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:cisco:unified_communications_manager:*:*:*:*:-:*:*:*;
cpe:2.3:a:cisco:unified_communications_manager:*:*:*:*:session_management:*:*:*;</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-918</td><td>T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-67038		Lantronix EDS5000 2.1.0.0R3 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:lantronix:eds5016:-:*:*:*:*:*:*:*	-
Lantronix EDS5000 Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1059.004: Command and Scripting Interpreter: Unix Shell, T1068: Exploitation for Privilege Escalation	https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/2538438657

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-34910		UniFi OS Server prior to 5.0.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ui:unifi_os_server:*:*:*:*:*:*:*:*	-
Ubiquiti UniFi OS Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-34909		UniFi OS Server prior to 5.0.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ui:unifi_os_server:*:*:*:*:*:*:*:*	-
Ubiquiti UniFi OS Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1083: File and Directory Discovery, T1552.001: Unsecured Credentials: Credentials In Files	https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-34908		UniFi OS Server prior to 5.0.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ui:unifi_os_server:*:*:*:*:*:*:*:*	-
Ubiquiti UniFi OS Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1548: Abuse Elevation Control Mechanism	https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20253		Splunk Enterprise versions 10.2.0–10.2.3 and 10.0.0–10.0.6	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:splunk:splunk:*:*:*:*:enterprise:*:*:*	-
Splunk Enterprise Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1505.003: Server Software Component: Web Shell	https://advisory.splunk.com/advisories/SVD-2026-0603

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-48907</td><td>  </td><td rowspan="2">Widget Factory Joomla Content Editor versions before 2.9.99.5</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:widgetfactorylimited:jce:*:*:*:*:*:*:joomla\!:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Widget Factory Joomla Content Editor Improper Access Control Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-284</td><td>T1190: Exploit Public-Facing Application, T1505.003: Server Software Component: Web Shell, T1059: Command and Scripting Interpreter</td><td>https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites</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-2026-54420</td><td>  </td><td rowspan="2">LiteSpeed cPanel Plugin (user-end) (Before 2.4.8), as distributed in LiteSpeed WHM Plugin (Before 5.3.2.0)</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:litespeedtech:litespeed_cpanel_plugin:*:*:*:*:*:*:*:*; cpe:2.3:a:litespeedtech:litespeed_whm_plugin:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following 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-61</td><td>T1068: Exploitation for Privilege Escalation, T1548: Abuse Elevation Control Mechanism, T1078: Valid Accounts</td><td>https://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20262		Cisco Catalyst SD-WAN Manager (releases 20.9.9.1 and earlier, 20.12.7.1 and earlier, 20.15.4.4 and earlier, 20.15.5.2 and earlier, 20.18.3, and 26.1.1.1 and earlier)	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-22	T1190: Exploit Public-Facing Application, T1505.003: Server Software Component: Web Shell, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-35273		Oracle PeopleSoft Enterprise PeopleTools: 8.61 and 8.62	ShinyHunters (aka UNC6240)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:*:*:*:*:*:*:*:*	-
Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1505.003: Server Software Component: Web Shell, T1657: Financial Theft	https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-10520		Ivanti Sentry (Before R10.5.2 / R10.6.2 / R10.7.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:standalone_sentry:*:*:*:*:*:*:*:*	-
Ivanti Sentry OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1505.003: Server Software Component: Web Shell	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-11645		Google Chrome (Before 149.0.7827.103)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium V8 Out-of-Bounds Read and Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1203: Exploitation for Client Execution, T1189: Drive-by Compromise	https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-7473		Arista EOS-based products:, 7020R Series, 7280R/R2Series, 7500R/R2 Series Limited exposure (IP-in-IPv6 and GUEv6) on: 7280R3 Series, 7500R3 Series, 7800R3 Series	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:arista:eos:*:*:*:*:*:*:*:*	-
Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1023	T1599: Network Boundary Bridging, T1046: Network Service Discovery	https://www.arista.com/en/support/advisories-notices/security-advisory/24005-security-advisory-0137

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20245		Cisco Catalyst SD-WAN 20.18.2.1 and earlier	UAT-8616
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-116	T1068: Exploitation for Privilege Escalation, T1136: Create Account, T1070.004: Indicator Removal: File Deletion	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx, https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-42271		BerriAI LiteLLM version 1.74.2 to before version 1.83.7	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:litellm:litellm:*:*:*:*:*:*:*:*	-
BerriAI LiteLLM Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1552.001: Unsecured Credentials: Credentials In Files	https://github.com/BerriAI/litellm/security/advisories/GHSA-v4p8-mg3p-g94g

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-50751		Check Point Mobile Access / SSL VPN, Remote Access VPN, Spark Firewall (R80.20.X, R80.40, R81, R81.10, R81.10.X, R81.20, R82, R82.00.X, R82.10)	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:o:checkpoint:gaia_os:*:*:*:*:*:*:*:*	Qilin Ransomware
Check Point Security Gateway Improper Authentication Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-287	T1133: External Remote Services, T1190: Exploit Public-Facing Application	https://support.checkpoint.com/results/sk/sk185033, https://blog.checkpoint.com/security/check-point-releases-important-hotfix-for-vulnerabilities-in-deprecated-ikev1-vpn-protocol/

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-28318</td><td>  </td><td rowspan="2">SolarWinds Serv-U 15.5.4 and below</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:solarwinds:serv-u:*:*:*:*:*:*:*:*; cpe:2.3:a:solarwinds:serv-u:15.5.4:-:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">SolarWinds Serv-U Uncontrolled Resource Consumption Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-400</td><td>T1190: Exploit Public-Facing Application, T1499.004: Endpoint Denial of Service: Application or System Exploitation</td><td>https://www.solarwinds.com/trust-center/security-advisories/CVE-2026-28318</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-2026-45247</td><td>  </td><td rowspan="2">Mirasvit Full Page Cache Warmer for Magento 2 before version 1.11.12</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:mirasvit:full_page_cache_warmer:*:*:*:*:*:magento:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Mirasvit Full Page Cache Warmer 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>T1190: Exploit Public-Facing Application, T1505.003: Server Software Component: Web Shell, T1056.003: Input Capture: Web Portal Capture</td><td>https://mirasvit.com/package/changelog/?package=mirasvit/module-cache-warmer&from=1.11.14</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-0492		Linux Kernel	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1611: Escape to Host, T1068: Exploitation for Privilege Escalation	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=24f6008564183aa120d07c03d9289519c2fe02af

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48595	✗	Android Framework	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:*:*:*:*:*:*:*:*	-
Android Framework Integer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1068: Exploitation for Privilege Escalation, T1203: Exploitation for Client Execution	https://source.android.com/docs/security/bulletin/2026/2026-06-01

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21182	✗	Oracle WebLogic Server versions 12.2.1.4.0 and 14.1.1.0.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:weblogic_server:*:*:*:*:*:*:*:*	-
Oracle WebLogic Server Unspecified Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1190: Exploit Public-Facing Application, T1005: Data from Local System	https://www.oracle.com/security-alerts/cpujul2024.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 26-04 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

July 02, 2026 • 04:00 AM

More at www.hivepro.com