Date of Publication
April 6, 2026

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

March 2026

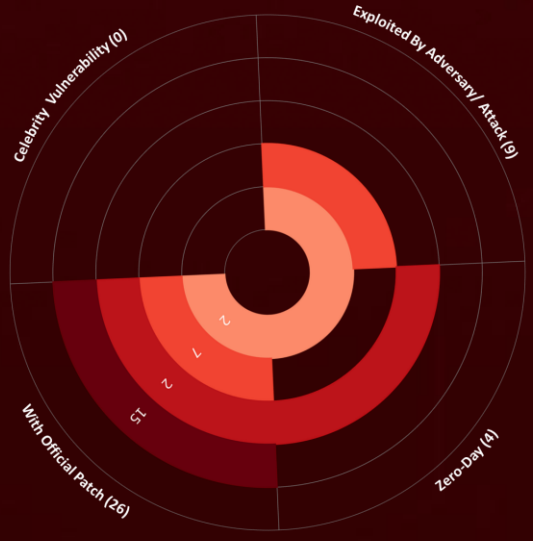
Table of Contents

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 **March 2026**, **26** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **4** are **zero-day** vulnerabilities; **9** have been **exploited** by a threat actor and employed in attacks.

26
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-3055	Citrix NetScaler Out-of-Bounds Read Vulnerability	Citrix NetScaler	9.3	✗	✓	April 02, 2026
CVE-2025-53521	F5 BIG-IP Stack-Based Buffer Overflow Vulnerability	F5 BIG-IP	9.8	✗	✓	March 30, 2026
CVE-2026-33634	Aquasecurity Trivy Embedded Malicious Code Vulnerability	Aquasecurity Trivy	8.8	✗	✓	April 09, 2026
CVE-2026-33017	Langflow Code Injection Vulnerability	Langflow Langflow	9.8	✗	✓	April 08, 2026
CVE-2025-32432	Craft CMS Code Injection Vulnerability	Craft CMS Craft CMS	10	✓	✓	April 03, 2026
CVE-2025-54068	Laravel Livewire Code Injection Vulnerability	Laravel Livewire	9.8	✗	✓	April 03, 2026
CVE-2025-43510	Apple Multiple Products Improper Locking Vulnerability	Apple Multiple Products	7.8	✗	✓	April 03, 2026
CVE-2025-43520	Apple Multiple Products Classic Buffer Overflow Vulnerability	Apple Multiple Products	5.5	✗	✓	April 03, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-31277	Apple Multiple Products Buffer Overflow Vulnerability	Apple Multiple Products	8.8			April 03, 2026
CVE-2026-20131	Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability	Cisco Secure Firewall Management Center (FMC)	10			March 22, 2026
CVE-2025-66376	Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	6.1			April 01, 2026
CVE-2026-20963	Microsoft SharePoint Deserialization of Untrusted Data Vulnerability	Microsoft SharePoint	9.8			March 21, 2026
CVE-2025-47813	Wing FTP Server Information Disclosure Vulnerability	Wing FTP Server Wing FTP Server	4.3			March 30, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-3910	Google Chromium V8 Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability	Google Chromium V8	8.8	✓	✓	March 27, 2026
CVE-2026-3909	Google Skia Out-of-Bounds Write Vulnerability	Google Skia	8.8	✓	✓	March 27, 2026
CVE-2025-68613	n8n Improper Control of Dynamically-Managed Code Resources Vulnerability	n8n n8n	8.8	✗	✓	March 25, 2026
CVE-2021-22054	Omnissa Workspace ONE Server-Side Request Forgery	Omnissa Workspace One UEM	7.5	✗	✓	March 23, 2026
CVE-2025-26399	SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability	SolarWinds Web Help Desk	9.8	✗	✓	March 12, 2026
CVE-2026-1603	Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability	Ivanti Endpoint Manager (EPM)	7.5	✗	✓	March 23, 2026
CVE-2017-7921	Hikvision Multiple Products Improper Authentication Vulnerability	Hikvision Multiple Products	9.8	✗	✓	March 26, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2021-22681	Rockwell Multiple Products Insufficient Protected Credentials Vulnerability	Rockwell Multiple Products	9.8			March 26, 2026
CVE-2023-43000	Apple Multiple products Use-After-Free Vulnerability	Apple Multiple Products	8.8			March 26, 2026
CVE-2021-30952	Apple Multiple Products Integer Overflow or Wraparound Vulnerability	Apple Multiple Products	7.8			March 26, 2026
CVE-2023-41974	Apple iOS and iPadOS Use-After-Free Vulnerability	Apple iOS and iPadOS	7.8			March 26, 2026
CVE-2026-22719	Broadcom VMware Aria Operations Command Injection Vulnerability	Broadcom VMware Aria Operations	8.1			March 24, 2026
CVE-2026-21385	Qualcomm Multiple Chipsets Memory Corruption Vulnerability	Qualcomm Multiple Chipsets	7.8			March 24, 2026

CVEs Details

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-3055</td><td>  </td><td rowspan="2">NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-60.58
NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-62.23
NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.262</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:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Citrix NetScaler Out-of-Bounds Read Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-125</td><td>T1190: Exploit Public-Facing Application T1212: Exploitation for Credential Access T1539: Steal Web Session Cookie</td><td>https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-53521		F5 BIG-IP APM	Highly Sophisticated Nation-State Threat Actor
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*	BRICKSTORM Backdoor
F5 BIG-IP Stack-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1190: Exploit Public-Facing Application T1505.003: Server Software Component: Web Shell T1059.004: Command & Scripting Interpreter: Unix Shell	https://my.f5.com/manage/s/article/K000156741

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-33634		Aquasecurity Trivy v0.69.4	TeamPCP
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:aquasec:setup-trivy:*:*:*:*:*:*:*:*	-
Aquasecurity Trivy Embedded Malicious Code Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1195.002: Supply Chain Compromise: Software Supply Chain T1552.001: Unsecured Credentials: Credentials in Files T1059.004: Command & Scripting Interpreter: Unix Shell	https://github.com/aquasecurity/trivy/discussions/10425; https://github.com/aquasecurity/trivy/security/advisories/GHSA-69fq-xp46-6x23

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-33017		Langflow Langflow version before 1.9.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:langflow:langflow:*:*:*:*:*:*:*:*	-
Langflow Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application T1059.006: Command & Scripting Interpreter: Python T1552.001: Unsecured Credentials: Credentials in Files	https://github.com/langflow-ai/langflow/releases; https://github.com/langflow-ai/langflow/security/advisories/GHSA-vwmf-pq79-vjvx

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32432		Craft CMS version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17	Mimo
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:craftcms:craft_cms:*:*:*:*:*:*:*:*	XMRig
Craft CMS Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application T1505.003: Server Software Component: Web Shell	https://github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-54068</td><td>  </td><td rowspan="2">Laravel Livewire v3.0.0-beta.1 – v3.6.3</td><td rowspan="2">MuddyWater</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:laravel:livewire:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Laravel Livewire 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>T1190: Exploit Public-Facing Application
T1059.006: Command & Scripting Interpreter: Python</td><td>https://github.com/livewire/livewire/commit/ef04be759da41b14d2d129e670533180a44987dc; https://github.com/livewire/livewire/security/advisories/GHSA-29cq-5w36-x7w3</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-43510	✗	Apple Multiple Products: iOS, iPadOS, macOS, watchOS, tvOS, visionOS	UNC6748, UNC6353
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*	GHOSTBLADE GHOSTKNIFE GHOSTSABER
Apple Multiple Products Improper Locking Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1189: Drive-by Compromise T1068: Exploitation for Privilege Escalation T1005: Data from Local System	https://support.apple.com/en-us/125632; https://support.apple.com/en-us/125633; https://support.apple.com/en-us/125634; https://support.apple.com/en-us/125635; https://support.apple.com/en-us/125636; https://support.apple.com/en-us/125637; https://support.apple.com/en-us/125638; https://support.apple.com/en-us/125639

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-43520	✗	Apple Multiple Products: iOS, iPadOS, macOS, watchOS, tvOS, visionOS	UNC6748, UNC6353
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*	GHOSTBLADE GHOSTKNIFE GHOSTSABER
Apple Multiple Products Classic Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1189: Drive-by Compromise T1068: Exploitation for Privilege Escalation T1005: Data from Local System	https://support.apple.com/en-us/125632; https://support.apple.com/en-us/125633; https://support.apple.com/en-us/125634; https://support.apple.com/en-us/125635; https://support.apple.com/en-us/125636; https://support.apple.com/en-us/125637; https://support.apple.com/en-us/125638; https://support.apple.com/en-us/125639

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-31277</td><td>✕</td><td rowspan="2">Apple Multiple Products: iOS, iPadOS, macOS, watchOS, tvOS, visionOS, Safari</td><td rowspan="2">UNC6748, UNC6353</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="3">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:visionos:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*</td><td rowspan="3">GHOSTBLADE
GHOSTKNIFE
GHOSTSABER</td></tr>
<tr><td rowspan="2">Apple Multiple Products Buffer Overflow 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>T1189: Drive-by Compromise
T1203: Exploitation for Client Execution
T1005: Data from Local System</td><td>https://support.apple.com/en-us/124147; https://support.apple.com/en-us/124149; https://support.apple.com/en-us/124152; https://support.apple.com/en-us/124153; https://support.apple.com/en-us/124154; https://support.apple.com/en-us/124155</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20131		Cisco Secure Firewall Management Center (FMC) - Multiple software versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:secure_firewall_management_center:6.4.0.13:*:*:*:*:*:*:*	Interlock ransomware
Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application T1059.007: Command & Scripting Interpreter: JavaScript T1486: Data Encrypted for Impact	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-66376		Synacor Zimbra Collaboration Suite (ZCS): Classic UI (XSS via CSS @import), Versions prior to Nov 2025 patch	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:*	-
Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1189: Drive-by Compromise T1557: Adversary-in-the-Middle T1114.002: Email Collection: Remote Email Collection	https://wiki.zimbra.com/wiki/Security_Center; https://wiki.zimbra.com/wiki/Zimbra_Releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20963		Microsoft SharePoint Server • Subscription Edition • SharePoint Server 2019 • SharePoint Enterprise Server 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:subscription:*:*:*	-
Microsoft SharePoint Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application T1505.003: Server Software Component: Web Shell T1210: Exploitation of Remote Services	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20963

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-47813		Wing FTP Server: All versions prior to 7.4.5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:wftpserver:wing_ftp_server:*:*:*:*:*:*:*:*	-
Wing FTP Server Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-209	T1190: Exploit Public-Facing Application T1087: Account Discovery T1552.001: Unsecured Credentials: Credentials in Files	https://www.wftpserver.com/download.htm

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-3910		Google Chrome (V8 Engine): All versions prior to 146.0.7680.75	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium V8 Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1189: Drive-by Compromise T1203: Exploitation for Client Execution T1059.007: Command & Scripting Interpreter: JavaScript	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-3909		Google Chrome (V8 Engine): All versions prior to 146.0.7680.75	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Skia Out-of-Bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1189: Drive-by Compromise T1203: Exploitation for Client Execution T1204.001: User Execution: Malicious Link	https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_13.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-68613		n8n Workflow Automation: v0.211.0 – v1.120.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:n8n:n8n:*:*:*:*:*:node.js:*:*	-
n8n Improper Control of Dynamically-Managed Code Resources Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-913	T1190: Exploit Public-Facing Application T1059: Command & Scripting Interpreter T1552.001: Unsecured Credentials: Credentials in Files	https://github.com/n8n-io/n8n/commit/08f332015153decdda3c37ad4fcb9f7ba13a7c79; https://github.com/n8n-io/n8n/commit/1c933358acef527ff61466e53268b41a04be1000; https://github.com/n8n-io/n8n/commit/39a2d1d60edde89674ca96dcbb3eb076ffff6316; https://github.com/n8n-io/n8n/security/advisories/GHSA-v98v-ff95-f3cp

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22054		Omnissa (fmr. VMware) Workspace ONE UEM	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:workspace_one_uem_console:*:*:*:*:*:*:*:*	-
Omnissa Workspace ONE Server-Side Request Forgery			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application T1018: Remote System Discovery T1552.001: Unsecured Credentials: Credentials in Files	https://www.vmware.com/security/advisories/VMSA-2021-0029.html; https://www.vmware.com/security/advisories/VMSA-2021-0029.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-26399		SolarWinds Web Help Desk: Versions prior to 12.8.7 HF1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:solarwinds:web_help_desk:*:*:*:*:*:*:*:*	-
SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application T1059: Command & Scripting Interpreter T1078: Valid Accounts	https://www.solarwinds.com/trust-center/security-advisories/CVE-2025-26399

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-1603		Ivanti Endpoint Manager (EPM): All versions prior to 2024 SU5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application T1552.001: Unsecured Credentials: Credentials in Files T1078.002: Valid Accounts: Domain Accounts	https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-7921		Hikvision IP Cameras & NVRs	Multiple Iranian Threat Actors
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:hikvision:ds-2cd2032-i_firmware:-:*:*:*:*:*:*:*	-
Hikvision Multiple Products Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application T1133: External Remote Services T1125: Video Capture	http://www.hikvision.com/us/about_10805.html; http://www.hikvision.com/us/about_10805.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22681		Rockwell Automation Multiple Products: Studio 5000 Logix Designer, Logix Controllers (multiple)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:rockwellautomation:factorytalk_services_platform:*:*:*:*:*:*:*:*	-
Rockwell Multiple Products Insufficient Protected Credentials Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-522	T0862: Supply Chain Compromise T0859: Valid Accounts T1552.004: Unsecured Credentials: Private Keys	https://www.rockwellautomation.com/es-es/trust-center/security-advisories/advisory.PN1550.html

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-43000</td><td>✗</td><td rowspan="2">Apple Multiple Products: iOS, iPadOS, macOS, watchOS, tvOS, Safari</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:apple:safari:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Apple Multiple products Use-After-Free Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-416</td><td>T1189: Drive-by Compromise
T1068: Exploitation for Privilege Escalation
T1005: Data from Local System</td><td>https://support.apple.com/en-us/120324; https://support.apple.com/en-us/120331; https://support.apple.com/en-us/120338; https://support.apple.com/en-us/126632</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-2021-30952</td><td>  </td><td rowspan="2">Apple Multiple Products: iOS, iPadOS, macOS, watchOS, tvOS, Safari</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:apple:safari:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Apple Multiple Products Integer Overflow or Wraparound Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-190</td><td>T1189: Drive-by Compromise
T1203: Exploitation for Client Execution
T1005: Data from Local System</td><td>https://support.apple.com/en-us/HT212975; https://support.apple.com/en-us/HT212976; https://support.apple.com/en-us/HT212978; https://support.apple.com/en-us/HT212980; https://support.apple.com/en-us/HT212982</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41974		Apple iOS / iPadOS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*	-
Apple iOS and iPadOS Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189: Drive-by Compromise T1068: Exploitation for Privilege Escalation T1005: Data from Local System	https://support.apple.com/en-us/120949; https://support.apple.com/en-us/126632; https://support.apple.com/en-us/HT213938; https://support.apple.com/kb/HT213938

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-22719</td><td>✗</td><td rowspan="2">Broadcom VMware Aria Operations (fmr. vROps): Aria Operations 8.x (before 8.18.6 patch), VMware Cloud Foundation 9.x</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="3">cpe:2.3:a:vmware:aria_operations:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*:*:*
cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:*</td><td rowspan="3">-</td></tr>
<tr><td rowspan="3">Broadcom VMware Aria Operations 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>T1190: Exploit Public-Facing Application
T1059: Command & Scripting Interpreter
T1078: Valid Accounts</td><td>https://knowledge.broadcom.com/external/article/430349; https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21385		Qualcomm Multiple Chipsets (Android): Multiple Snapdragon SoCs	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qualcomm:sm7675p_firmware:-:*:*:*:*:*:*:*	-
Qualcomm Multiple Chipsets Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1190: Exploit Public-Facing Application T1068: Exploitation for Privilege Escalation T1005: Data from Local System	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2026-bulletin.html; https://source.android.com/docs/security/bulletin/2026/2026-03-01

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.

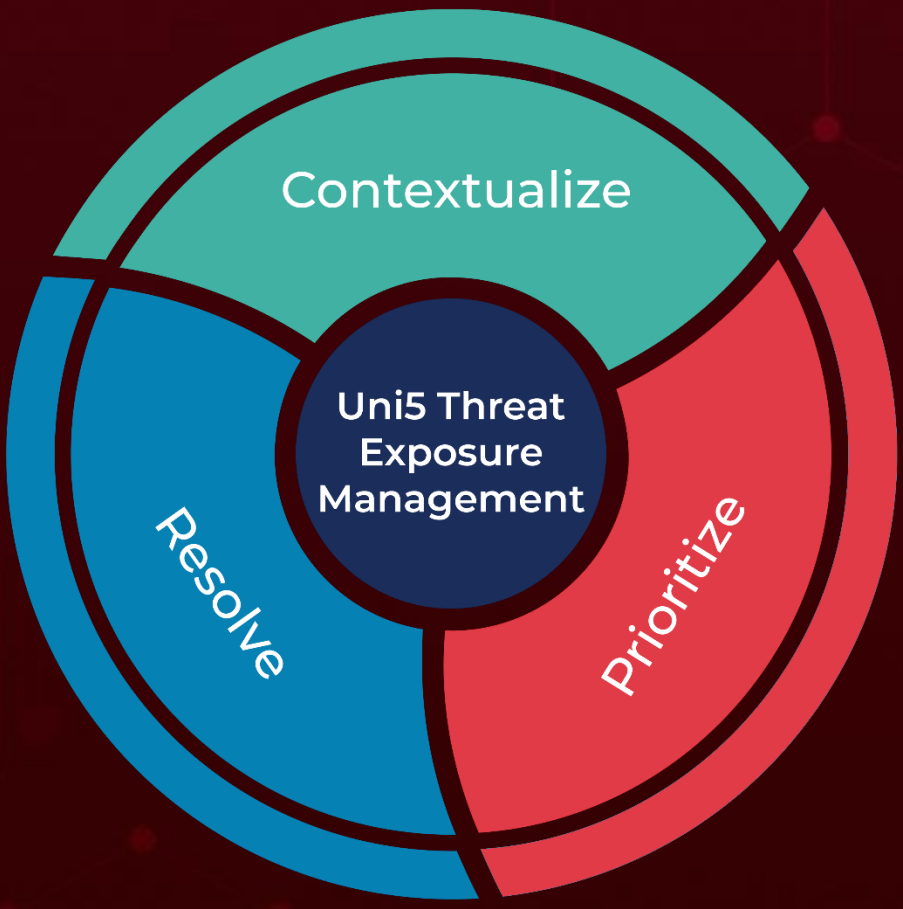
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

April 06, 2026 • 11:35 PM

More at www.hivepro.com