Date of Publication
February 3, 2026

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

January 2026

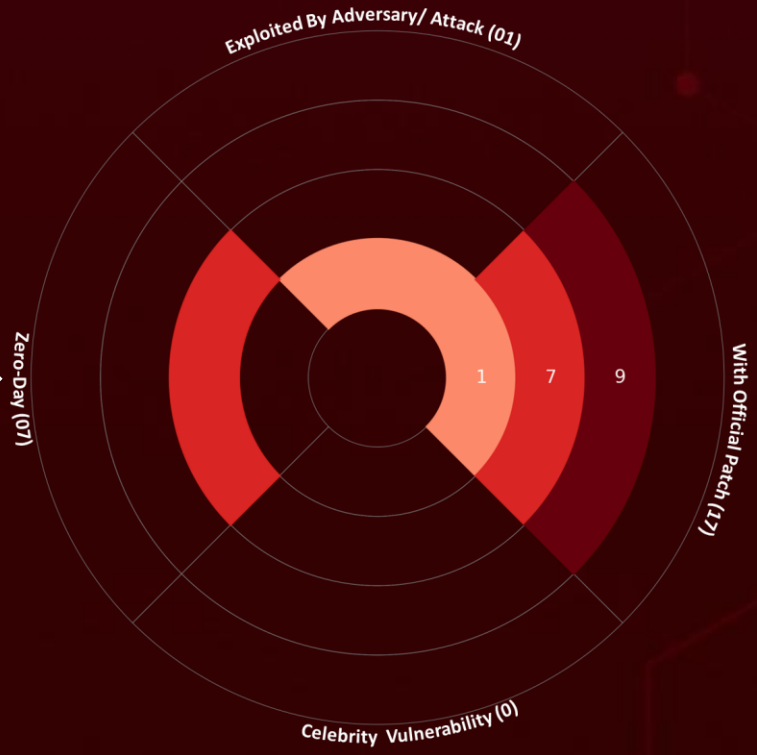
Table of Contents

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 January 2026, **17** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **seven** are **zero-day** vulnerabilities; **one** has been **exploited** by a threat actor and employed in attacks.

17
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-1281	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	9.8	✓	✓	February 1, 2026
CVE-2026-24858	Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability	Fortinet Multiple Products	9.8	✓	✓	January 30, 2026
CVE-2018-14634	Linux Kernel Integer Overflow Vulnerability	Linux Kernal	7.8	✗	✓	February 16, 2026
CVE-2025-52691	SmarterTools SmarterMail Unrestricted Upload of File with Dangerous Type Vulnerability	SmarterTools SmarterMail	10	✗	✓	February 16, 2026
CVE-2026-23760	SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability	SmarterTools SmarterMail	9.8	✗	✓	February 16, 2026
CVE-2026-24061	GNU InetUtils Argument Injection Vulnerability	GNU InetUtils	9.8	✗	✓	February 16, 2026
CVE-2026-21509	Microsoft Office Security Feature Bypass Vulnerability	Microsoft Office	7.8	✓	✓	February 16, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2024-37079	Broadcom VMware vCenter Server Out-of-bounds Write Vulnerability	Broadcom VMware vCenter Server	9.8	✗	✓	February 13, 2026
CVE-2025-68645	Synacor Zimbra Collaboration Suite (ZCS) PHP Remote File Inclusion Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	8.8	✗	✓	February 12, 2026
CVE-2025-34026	Versa Concerto Improper Authentication Vulnerability	Versa Concerto	7.5	✗	✓	February 12, 2026
CVE-2025-31125	Vite Vitejs Improper Access Control Vulnerability	Vite Vitejs	7.5	✗	✓	February 12, 2026
CVE-2025-54313	Prettier eslint-config-prettier Embedded Malicious Code Vulnerability	Prettier eslint-config-prettier	7.5	✗	✓	February 12, 2026
CVE-2026-20045	Cisco Unified Communications Products Code Injection Vulnerability	Cisco Unified Communications Manager	9.8	✓	✓	February 11, 2026
CVE-2026-20805	Microsoft Windows Information Disclosure Vulnerability	Microsoft Windows	5.5	✓	✓	February 3, 2026
CVE-2025-8110	Gogs Path Traversal Vulnerability	Gogs	8.8	✓	✓	February 2, 2026
CVE-2009-0556	Microsoft Office PowerPoint Code Injection Vulnerability	Microsoft Office	8.8	✓	✓	January 28, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2025-37164	Hewlett Packard Enterprise (HPE) OneView Code Injection Vulnerability	Hewlett Packard Enterprise (HPE) OneView	9.8			January 28, 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-2026-1281</td><td>  </td><td rowspan="2">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</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: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:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Ivanti Endpoint Manager Mobile (EPMM) 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: Command and Scripting Interpreter</td><td>https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US</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="4">CVE-2026-24858</td><td>  </td><td rowspan="2">Fortinet FortiOS (Before 7.0.19, 7.2.13, 7.4.11, 7.6.6) Fortinet FortiManager (Before 7.0.16, 7.2.13, 7.4.10, 7.6.6) Fortinet FortiAnalyzer (Before 7.0.16, 7.2.12, 7.4.10, 7.6.6) Fortinet FortiProxy (7.0, 7.2, Before 7.4.13, 7.6.6)</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:fortinet:fortios:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortimanager:*:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortianalyzer:*:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability</td><td>  </td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td></td><td>CWE-288</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1136: Create Account, T1005: Data from Local System</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-26-060, https://docs.fortinet.com/upgrade-tool/fortigate</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-14634	✗	Linux Kernel versions 2.6.x, 3.10.x and 4.14.x, RedHat	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux_desktop:*:*:*:*:*:*:*:*	-
Linux Kernel Integer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1068: Exploitation for Privilege Escalation	https://access.redhat.com/security/cve/cve-2018-14634

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-52691	✗	SmarterTools SmarterMail	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:smartertools:smartermail:*:*:*:*:*:*:*:*	-
SmarterTools SmarterMail Unrestricted Upload of File with Dangerous Type Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1505: Server Software Component, T1505.003: Web Shell, T1059: Command and Scripting Interpreter	https://www.smartertools.com/smartermail/release-notes/current

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-23760</td><td>  </td><td rowspan="2">SmarterTools SmarterMail versions prior to build 9511</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:smartertools:smartermail:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-288</td><td>T1190: Exploit Public-Facing Application, T1078: Valid Accounts</td><td>https://www.smartertools.com/smartermail/release-notes/current</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-24061	✗	GNU InetUtils telnetd versions 1.9.3 - 2.7	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gnu:inetutils:*:*:*:*:*:*:*:*	-
GNU InetUtils Argument Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-88	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter, T1098: Account Manipulation, T1082: System Information Discovery	https://codeberg.org/inetutils/inetutils/commit/fd702c02497b2f398e739e3119bed0b23dd7aa7b, https://codeberg.org/inetutils/inetutils/commit/ccba9f748aa8d50a38d7748e2e60362edd6a32cc, https://cgit.git.savannah.gnu.org/cgit/inetutils.git

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21509	✗	Microsoft Office 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	-
Microsoft Office Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-807	T1566: Phishing, T1204: User Execution, T1559: Inter-Process Communication, T1562: Impair Defenses	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-37079		vCenter Server: 7.0 U1 - 8.0.0c Cloud Foundation versions 4.x and 5.x.	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:*	-
Broadcom VMware vCenter Server Out-of-bounds Write Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINKS**
	CWE-122	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u2d-release-notes/index.html ,https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-vcenter-server-80u1e-release-notes/index.html ,https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u3r-release-notes/index.html ,https://knowledge.broadcom.com/external/article?legacyId=88287

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-68645	✗	Zimbra Collaboration (ZCS) Webmail Classic UI 10.0 and 10.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:*	-
Synacor Zimbra Collaboration Suite (ZCS) PHP Remote File Inclusion Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-98	T1083: File and Directory Discovery	https://wiki.zimbra.com/wiki/Security_Center, https://wiki.zimbra.com/wiki/Zimbra_Responsible_Disclosure_Policy

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTORS
CVE-2025-34026	✗	Versa Concerto from 12.1.2 through 12.2.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:versa-networks:concerto:*:*:*:*:*:*:*:*	-
Versa Concerto Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1078: Valid Accounts	https://security-portal.versa-networks.com/emailbulletins/6830f94328defa375486ff2e

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-31125	✗	Vite Vitejs	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vitejs:vite:*:*:*:*:*:node.js:*:*	-
Vite Vitejs Improper Access Control Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200, CWE-284	T1083: File and Directory Discovery, T1005: Data from Local System, T1068: Exploitation for Privilege Escalation	https://github.com/vitejs/vite/commit/59673137c45ac2bcfad1170d954347c1a17ab949

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTORS
CVE-2025-54313	✗	Prettier eslint-config-prettier 8.10.1, 9.1.1, 10.1.6, and 10.1.7	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:prettier:eslint-config-prettier:*:*:*:*:*:node.js:*:*	-
Prettier eslint-config-prettier Embedded Malicious Code Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1195: Supply Chain Compromise, T1195.002: Compromise Software Supply Chain	https://github.com/prettier/eslint-config-prettier/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-2026-20045</td><td>  </td><td rowspan="2">Cisco Unified Communications Manager, Unified Communications Manager Session Management Edition, Unified Communications Manager IM & Presence Service, Unity Connection, Webex Calling Dedicated Instance: versions before 14SU5, 15SU4</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:cisco:unified_communications_manager:*:*:*:*:*:*:*:*
cpe:2.3:a:cisco:unified_communications_manager_session_management_edition:*:*:*:*:*:*:*:*
cpe:2.3:a:cisco:unified_communications_manager_im_and_presence_service:*:*:*:*:*:*:*:*
cpe:2.3:a:cisco:unity_connection:*:*:*:*:*:*:*:*
cpe:2.3:a:cisco:webex_calling_dedicated_instance:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Cisco Unified Communications Products 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: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20805	✗ ZERO-DAY	Windows 10 - 11 25H2, Windows Server 2012, 2016, 2019, 2025, 2022	-
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	-
Microsoft Windows Information Disclosure Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-502	T1190: Exploit Public-Facing Application, T1059.006: Python, T1082: System Information Discovery, T1588.007: Artificial Intelligence	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-20805

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTORS
CVE-2025-8110	✗ ZERO-DAY	Gogs (Prior to 0.13.4, all versions through 0.13.3)	-
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:gogs:gogs:*:*:*:*:*:*:*:*	-
Gogs Path Traversal Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-22	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1505: Server Software Component	https://github.com/gogs/gogs/commit/553707f3fd5f68f47f531cfcff56aa3ec294c6f6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2009-0556	✗	Microsoft Office PowerPoint 2000 SP3, 2002 SP3, and 2003 SP3, and PowerPoint in Microsoft Office 2004 for Mac	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:office_powerpoint:*:*:*:*:*:*:*:*	-
Microsoft Office PowerPoint Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-017

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-37164	✗	HPE OneView (Before 11.0)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:hpe:oneview:*:*:*:*:*:*:*:*	RondoDox Botnet
Hewlett Packard Enterprise (HPE) OneView Code Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US, https://myenterpriselicense.hpe.com/cwp-ui/product-details/HPE_OV_CVE_37164_Z7550-98077/-/sw_free, https://support.hpe.com/connect/s/softwaredetails?collectionId=MTX-64daeb5ed0df44a0&tab=releaseNotes

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.

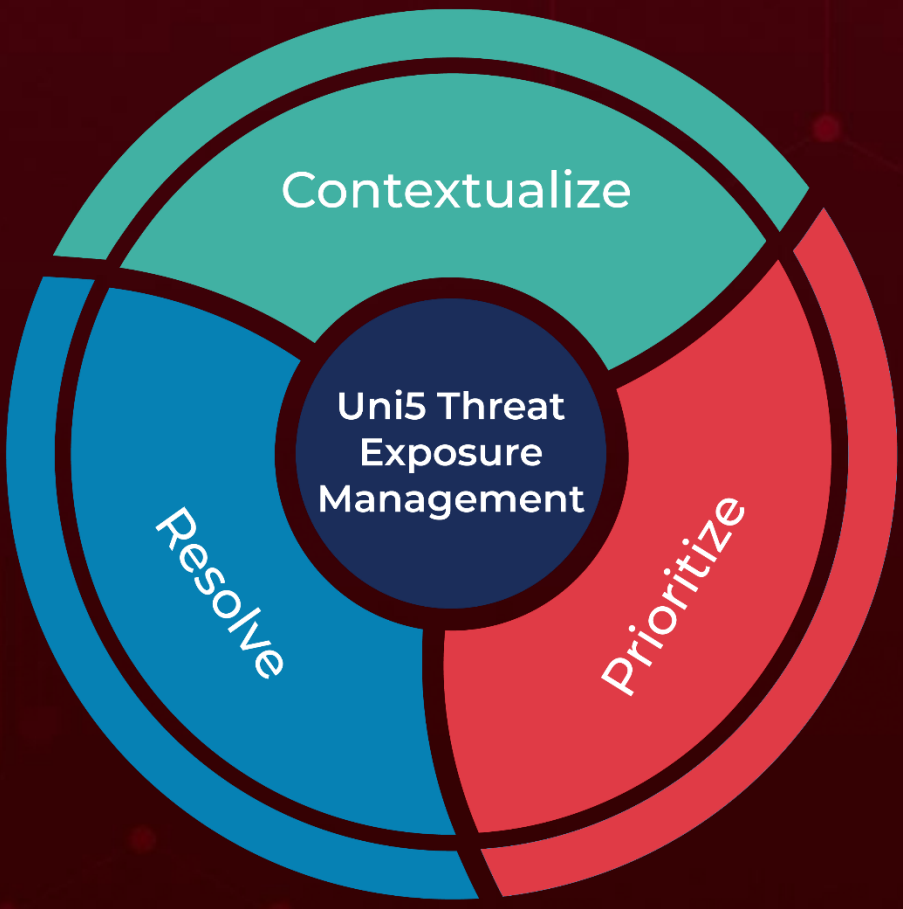
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

February 3, 2026 • 4:30 AM

More at www.hivepro.com