Date of Publication
March 2, 2026

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

February 2026

Table of Contents

Summary 03

CVEs List 04

CVEs Details 07

Recommendations 21

References 22

Appendix 22

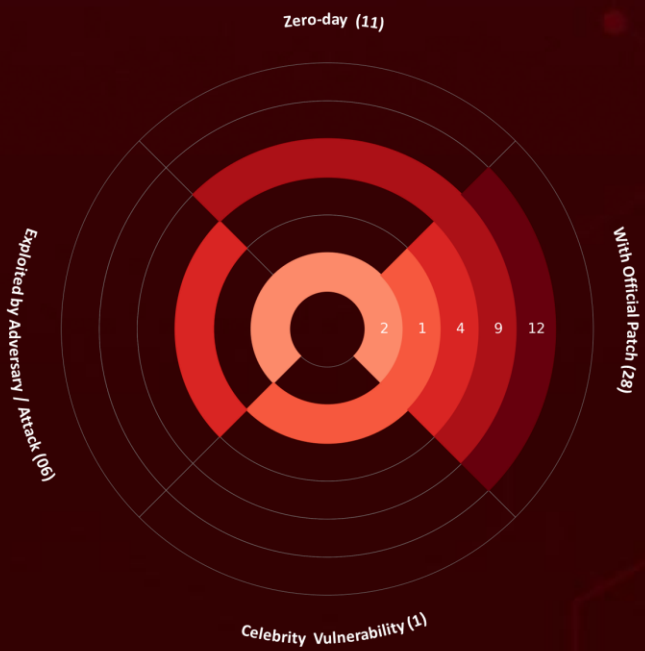
What Next? 23

Summary

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

It is recommended that all organizations review and monitor the KEV catalog, prioritize remediation of listed vulnerabilities, and reduce the likelihood of compromise by threat actors. In **February 2026**, **28** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **11** are **zero-day** vulnerabilities; **6** have been **exploited** by a threat actor and employed in attacks.

28
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2022-20775	Cisco SD-WAN Path Traversal Vulnerability	Cisco SD-WAN	7.8	✗	✓	February 27, 2026
CVE-2026-20127	Cisco Catalyst SD-WAN Controller and Manager Authentication Bypass Vulnerability	Cisco Catalyst SD-WAN Controller and Manager	10	✓	✓	February 27, 2026
CVE-2026-25108	Soliton Systems K.K FileZen OS Command Injection Vulnerability	Soliton Systems K.K FileZen	8.7	✗	✓	March 17, 2026
CVE-2025-49113	RoundCube Webmail Deserialization of Untrusted Data Vulnerability	RoundCube Webmail	8.8	✗	✓	March 13, 2026
CVE-2025-68461	RoundCube Webmail Cross-site Scripting Vulnerability	RoundCube Webmail	6.1	✗	✓	March 13, 2026
CVE-2021-22175	GitLab Server-Side Request Forgery (SSRF) Vulnerability	GitLab	9.8	✗	✓	March 11, 2026
CVE-2026-22769	Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability	Dell RecoverPoint for Virtual Machines (RP4VMs)	10	✓	✓	February 21, 2026
CVE-2020-7796	Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	9.8	✗	✓	March 10, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-7694	TeamT5 ThreatSonar Anti-Ransomware Unrestricted Upload of File with Dangerous Type Vulnerability	TeamT5 ThreatSonar Anti-Ransomware	7.2	✗	✓	March 10, 2026
CVE-2008-0015	Microsoft Windows Video ActiveX Control Remote Code Execution Vulnerability	Microsoft Windows	8.8	✓	✓	March 10, 2026
CVE-2026-2441	Google Chromium CSS Use-After-Free Vulnerability	Google Chromium CSS	8.8	✓	✓	March 10, 2026
CVE-2026-1731	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability	BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA)	9.8	✗	✓	February 16, 2026
CVE-2026-20700	Apple Multiple Buffer Overflow Vulnerability	Apple	7.8	✓	✓	March 05, 2026
CVE-2024-43468	Microsoft Configuration Manager SQL Injection Vulnerability	Microsoft Configuration Manager	9.8	✗	✓	March 05, 2026
CVE-2025-15556	Notepad++ Download of Code Without Integrity Check Vulnerability	Notepad++	7.5	✗	✓	March 05, 2026
CVE-2025-40536	SolarWinds Web Help Desk Security Control Bypass Vulnerability	SolarWinds Web Help Desk	9.8	✗	✓	February 15, 2026
CVE-2026-21513	Microsoft MSHTML Framework Protection Mechanism Failure Vulnerability	Microsoft MSHTML Framework	8.8	✓	✓	March 03, 2026
CVE-2026-21525	Microsoft Windows NULL Pointer Dereference Vulnerability	Microsoft Windows	6.2	✓	✓	March 03, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-21510	Microsoft Windows Shell Protection Mechanism Failure Vulnerability	Microsoft Windows	8.8	✓	✓	March 03, 2026
CVE-2026-21533	Microsoft Windows Improper Privilege Management Vulnerability	Microsoft Windows	7.8	✓	✓	March 03, 2026
CVE-2026-21519	Microsoft Windows Type Confusion Vulnerability	Microsoft Windows	7.8	✓	✓	March 03, 2026
CVE-2026-21514	Microsoft Office Word Reliance on Untrusted Inputs in a Security Decision Vulnerability	Microsoft Office Word	7.8	✓	✓	March 03, 2026
CVE-2025-11953	Metro4Shell (React Native Community CLI OS Command Injection Vulnerability)	React Native Community CLI	9.8	✗	✓	February 26, 2026
CVE-2026-24423	SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability	SmarterTools SmarterMail	9.8	✗	✓	February 26, 2026
CVE-2021-39935	GitLab Community and Enterprise Editions Server-Side Request Forgery (SSRF) Vulnerability	GitLab Community and Enterprise Editions	7.5	✗	✓	February 24, 2026
CVE-2025-64328	Sangoma FreePBX OS Command Injection Vulnerability	Sangoma FreePBX	7.2	✗	✓	February 24, 2026
CVE-2019-19006	Sangoma FreePBX Improper Authentication Vulnerability	Sangoma FreePBX	9.8	✗	✓	February 24, 2026
CVE-2025-40551	SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability	SolarWinds Web Help Desk	9.8	✗	✓	February 06, 2026

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-20775	✗	Cisco SD-WAN Software (Before 20.6.3 to 20.6.4)	UAT-8616
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:catalyst_sd-wan_controller:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	-
Cisco SD-WAN Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-25, CWE-282	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20127	✗	Cisco Catalyst SD-WAN Controller & SD-WAN Manager (Before 20.9.8.2, 20.12.6.1, 20.12.5.3, 20.12.6.1, 20.15.4.2, 20.15.4.2, 20.15.4.2, 20.18.2.1, 20.18.2.1)	UAT-8616
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:sd-wan:*:*:*:*:*:*:*:*	-
Cisco Catalyst SD-WAN Controller and Manager Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-25108		FileZen V4.2.1 to 5.0.10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:soliton:filezen:*:*:*:*:*:*:*:*	-
Soliton Systems K.K FileZen OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.soliton.co.jp/support/2026/006657.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-49113		Roundcube Webmail Versions before 1.5.10 and 1.6.x before 1.6.11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
RoundCube Webmail Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/roundcube/roundcubemail/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-68461	✗	Roundcube Webmail before 1.5.12 and 1.6 before 1.6.12	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
RoundCube Webmail Cross-site Scripting Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/roundcube/roundcubemail/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22175	✗	GitLab All Versions from 10.5	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	-
GitLab Server-Side Request Forgery (SSRF) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1059: Command and Scripting Interpreter	https://about.gitlab.com/releases/categories/releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-22769		Dell RecoverPoint for Virtual Machines, versions prior to 6.0.3.1 HF1	UNC6201
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:dell:recoverpoint_for_virtual_machines:*:*:*:*:*:*:*:*	BRICKSTORM GRIMBOLT SLAYSTYLE
Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-798	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://www.dell.com/support/kbdoc/en-in/000426773/dsa-2026-079

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-7796		Zimbra Collaboration Suite (ZCS) before 8.8.15 Patch 7	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:*	-
Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1059: Command and Scripting Interpreter	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7694		ThreatSonar Anti-Ransomware version 3.4.5 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:teamt5:threatsonar_anti-ransomware:*:*:*:*:*:*:*:*	-
TeamT5 ThreatSonar Anti-Ransomware Unrestricted Upload of File with Dangerous Type Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://teamt5.org/en/posts/vulnerability-notice-threat-sonar-anti-ransomware-20240715/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2008-0015		Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista (Gold, SP1, and SP2), and Windows Server 2008 (Gold and SP2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_2003_server:-:sp2:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_2003_server:-:sp2:itanium:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_2003_server:-:sp2:x64:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_xp:*:sp2:professional_x64:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_xp:-:sp2:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_xp:-:sp3:*:*:*:*:*:*:*	-
Microsoft Windows Video ActiveX Control Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119, CWE-121	T1059: Command and Scripting Interpreter	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-032

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-2441		Google Chrome (Before 145.0.7632.75 on Windows/macOS; Before 144.0.7559.75 on Linux)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium CSS Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1189: Drive-By Compromise, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-1731		BeyondTrust Remote Support: Before 25.3.2 BeyondTrust Privileged Remote Access: Before 25.1.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*:* cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*:*	-
BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.beyondtrust.com/trust-center/security-advisories/bt26-02

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20700		Apple iOS (Before26.3), Apple iPadOS (Before 26.3), Apple macOS Tahoe (Before 26.3), Apple tvOS (Before 26.3), Apple watchOS (Before 26.3), Apple visionOS (Before 26.3)	-
	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:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*	-
Apple Multiple Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1189: Drive-by Compromise, T1068: Exploitation for Privilege Escalation, T1574: Hijack Execution Flow, T1574.004: Dylib Hijacking	https://support.apple.com/en-us/126346, https://support.apple.com/en-us/126348, https://support.apple.com/en-us/126351, https://support.apple.com/en-us/126352, https://support.apple.com/en-us/126353

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43468		Microsoft Configuration Manager: 2303, 2309, 2403	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:configuration_manager:*:*:*:*:*:*:*:*	-
Microsoft Configuration Manager SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-15556		Notepad++ versions prior to 8.8.9	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:notepad-plus-plus:notepad\+\+:*:*:*:*:*:*:*:*	-
Notepad++ Download of Code Without Integrity Check Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-494	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://github.com/notepad-plus-plus/notepad-plus-plus/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-40536		SolarWinds Web Help Desk 12.8.8 HF1 and all previous versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:solarwinds:web_help_desk:*:*:*:*:*:*:*:*	-
SolarWinds Web Help Desk Security Control Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://documentation.solarwinds.com/en/success_center/whd/content/release_notes/whd_2026-1_release_notes.htm

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21513		Windows 10, 11 26H1 Windows Server 2012, 2016, 2025, 2022, 2019	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft MSHTML Framework Protection Mechanism Failure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1204: User Execution, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21513

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21525		Windows 10, 11 26H1 Windows Server 2012, 2016, 2025, 2022, 2019	-
	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 NULL Pointer Dereference Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-476	T1499: Endpoint Denial of Service	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21525

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21510		Windows 10, 11 25H2 Windows Server 2012, 2016, 2025, 2022, 2019	-
	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 Shell Protection Mechanism Failure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1204.001: Malicious Link, T1204: User Execution	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21510

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21533		Windows 10, 11 25H2 Windows Server 2012, 2016, 2025, 2022, 2019	-
	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 Improper Privilege Management Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21533

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21519		Windows 10,11 25H2 Windows Server 2016, 2025, 2022, 2019	-
	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 Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21519

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21514		Microsoft Office Word	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office_long_term_servicing_channel:*:*:*:*:*	-
Microsoft Office Word Reliance on Untrusted Inputs in a Security Decision Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-807	T1566: Phishing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21514

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-11953	Metro4Shell	React Native Community CLI versions 4.8.0 through 19.1.1 and version 18.0.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:react-native-community:react_native_community_cli:*:*:*:*:*:*:*:*	-
React Native Community CLI OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://github.com/react-native-community/cli/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-24423		SmarterTools SmarterMail (Before Build 9511)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:smartertools:smartermail:*:*:*:*:*:*:*:*	Warlock ransomware
SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.smartertools.com/smartermail/release-notes/current

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-39935	✗	GitLab CE/EE affecting versions 10.5 before 14.3.6, 14.4 before 14.4.4, and 14.5 before 14.5.2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	-
GitLab Community and Enterprise Editions Server-Side Request Forgery (SSRF) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1068: Exploitation for Privilege Escalation	https://about.gitlab.com/releases/categories/releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-64328	✗	FreePBX Endpoint Manager versions 17.0.2.36 and above before 17.0.3	INJ3CTOR3
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sangoma:firestore:*:*:*:*:*:freepbx:*:*	EncystPHP
Sangoma FreePBX OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.freepbx.org/downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-19006		Sangoma FreePBX 115.0.16.26 and below, 14.0.13.11 and below, 13.0.197.13 and below	INJ3CTOR3
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sangoma:freepbx:*:*:*:*:*:*:*:*	-
Sangoma FreePBX Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1059: Command and Scripting Interpreter	https://www.freepbx.org/downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-40551		Web Help Desk 12.8.8 HF1 and below	-
	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	T1059: Command and Scripting Interpreter	https://documentation.solarwinds.com/en/success_center/whd/content/release_notes/whd_2026-1_release_notes.htm#link4

Recommendations

- To ensure the security of their systems and data, organizations should prioritize the vulnerabilities listed above and promptly apply patches to them before the due date provided.

- It is essential to comply with BINDING OPERATIONAL DIRECTIVE 22-01 provided by the Cyber security and Infrastructure Security Agency (CISA). This directive outlines the minimum cybersecurity standards that all federal agencies must follow to protect their organization from cybersecurity threats.

- The affected products listed in the report can help organizations identify assets that have been affected by KEVs, even without conducting a scan. These assets should be patched with priority to reduce the risk.

References

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Appendix

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

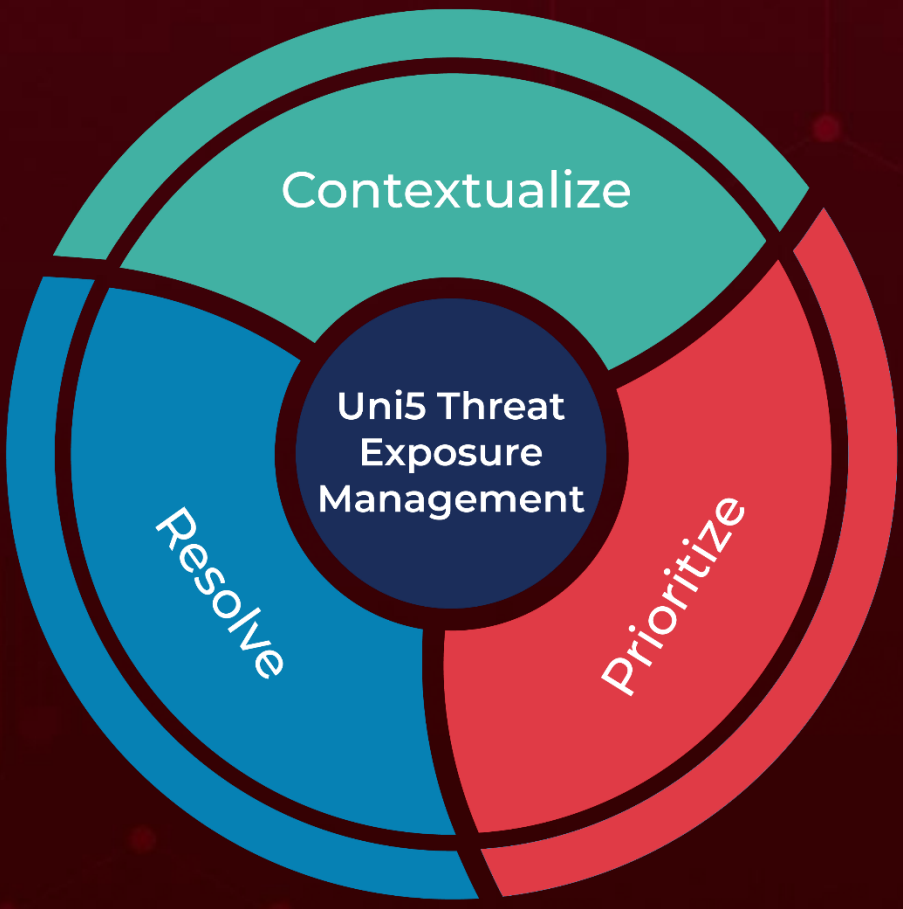
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

Due Date: The "Due Date" provided by CISA is a recommended deadline that organizations should use to prioritize the remediation of identified vulnerabilities in their systems, with the aim of enhancing their overall security posture.

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.



REPORT GENERATED ON

March 02, 2026 • 11:50 PM

More at www.hivepro.com