



HiveForce Labs

CISA

KNOWN

EXPLOITED

VULNERABILITY

CATALOG

July 2026

Table of Contents

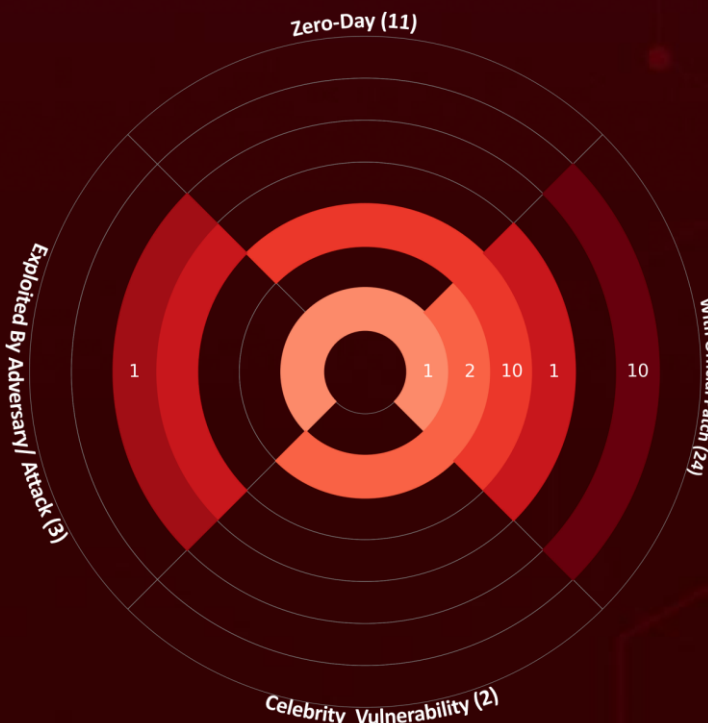
<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	10
<u>Recommendations</u>	30
<u>References</u>	31
<u>Appendix</u>	31
<u>What Next?</u>	32

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 **July 2026**, **26** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **11** are **zero-day** vulnerabilities; **3** 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
<u>CVE-2026-20316</u>	Cisco Secure Firewall Management Center Use of Hard-coded Password Vulnerability	Cisco Secure Firewall Management Center (FMC)	5.3			August 01, 2026
CVE-2025-68686	Fortinet FortiOS Exposure of Sensitive Information to an Unauthorized Actor Vulnerability	Fortinet FortiOS	5.9			August 10, 2026
<u>CVE-2026-16812</u>	Arista VeloCloud Orchestrator On-Prem OS Command Injection Vulnerability	Arista VeloCloud Orchestrator	10			July 30, 2026
<u>CVE-2026-16232</u>	Check Point SmartConsole Improper Authentication Vulnerability	Check Point SmartConsole	9.1			July 25, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-50522	Microsoft SharePoint Deserialization of Untrusted Data Vulnerability	Microsoft SharePoint	9.8			July 25, 2026
CVE-2026-60137	WordPress Core SQL Injection Vulnerability	WordPress Core	5.9			August 04, 2026
CVE-2026-63030	WordPress Core Interpretation Conflict Vulnerability	WordPress Core	9.8			July 24, 2026
CVE-2026-0770	Langflow Inclusion of Functionality from Untrusted Control Sphere Vulnerability	Langflow	9.8			July 24, 2026
CVE-2021-27137	DD-WRT Stack-Based Buffer Overflow Vulnerability	DD-WRT	8.1			July 24, 2026
CVE-2026-58644	Microsoft SharePoint Deserialization of Untrusted Data Vulnerability	Microsoft SharePoint	9.8			July 19, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-25089	Fortinet FortiSandbox OS Command Injection Vulnerability	Fortinet FortiSandbo x	9.8			July 19, 2026
CVE-2026-39808	Fortinet FortiSandbox OS Command Injection Vulnerability	Fortinet FortiSandbo x	9.8			July 19, 2026
CVE-2026-46817	Oracle E-Business Suite Improper Privilege Management Vulnerability	Oracle E-Business Suite	9.8			July 18, 2026
CVE-2023-4346	KNX Association KNX Protocol Connection Authorization Option 1 Overly Restrictive Account Lockout Mechanism Vulnerability	KNX Association KNX Protocol Connection Authorization Option 1	7.5			July 29, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
<u>CVE-2026-56155</u>	Microsoft Active Directory Federation Services Insufficient Granularity of Access Control Vulnerability	Microsoft Active Directory Federation Services	7.8			July 28, 2026
<u>CVE-2026-56164</u>	Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability	Microsoft SharePoint Server	9.8			July 17, 2026
<u>CVE-2026-15409</u>	SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability	SonicWall SMA1000 Appliances	10			July 17, 2026
<u>CVE-2026-15410</u>	SonicWall SMA1000 Appliances Code Injection Vulnerability	SonicWall SMA1000 Appliances	7.2			July 17, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2008-4128	Cisco IOS Cross-Site Request Forgery Vulnerability	Cisco IOS	4.3			July 16, 2026
<u>CVE-2026-56291</u>	Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability	Balbooa Forms	9.8			July 13, 2026
CVE-2026-48939	iCagenda Unrestricted Upload of File with Dangerous Type Vulnerability	iCagenda	9.8			July 13, 2026
CVE-2026-48908	JoomShaper SP Page Builder Unrestricted Upload of File with Dangerous Type Vulnerability	JoomShaper SP Page Builder	9.8			July 10, 2026
CVE-2026-55255	Langflow Authorization Bypass Through User-Controlled Key Vulnerability	Langflow	8.4			July 10, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-56290	Joomla Page Builder Improper Access Control Vulnerability	Joomla Page Builder	9.8			July 10, 2026
<u>CVE-2026-48282</u>	Adobe ColdFusion Path Traversal Vulnerability	Adobe ColdFusion	10			July 10, 2026
<u>CVE-2026-45659</u>	Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability	Microsoft SharePoint Server	8.8			July 04, 2026

 CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-20316</u>		Cisco Secure Firewall Management Center (FMC) Software (7.0.x through 7.7.x and 10.0.x releases prior to the fixed hot-fix builds)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:secure_firewall_management_center:*:*:*:*:*:*	-
Cisco Secure Firewall Management Center Use of Hard-coded Password Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-259	T1078: Valid Accounts, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-fmc-static-cred-BET3Cjh

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-68686		Fortinet FortiOS 7.6.0 through 7.6.1, FortiOS 7.4.0 through 7.4.6, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	-
Fortinet FortiOS Exposure of Sensitive Information to an Unauthorized Actor Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1211: Exploitation for Defense Evasion, T1005: Data from Local System	https://fortiguard.fortinet.com/psirt/FG-IR-25-934

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-16812</u>		Arista VeloCloud Orchestrator (VCO) On- Prem (5.2.x before 5.2.3.14, 6.1.x before 6.1.3.4, 6.4.x before 6.4.2.4, 7.0.x before 7.0.0.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*:*	-
Arista VeloCloud Orchestrator On-Prem OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-16232</u>		Check Point Security Management Server/ Multi Domain Security Management (R77.30, R80, R80.10, R80.20, R80.30, R81 R81.10, R81.20, R82, R82.10)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:checkpoint:multi-domain_security_management:*.*.*.*.*.*.*.*	-
Check Point SmartConsole Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application,T1550: Use Alternate Authentication Material, T1550.001: Application Access Token	https://support.checkpoint.com/results/sk/sk185169/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-50522</u>		Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*	-
Microsoft SharePoint Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-60137</u>	wp2shell	WordPress Core (Version before 6.9.5 and 7.0.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*	-
WordPress Core SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application	https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-63030</u>	wp2shell	WordPress Core (Version before 6.9.5 and 7.0.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:wordpress:wordpress:*.~*~*~*~*~*~*	-
WordPress Core Interpretation Conflict Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-436	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-0770		Langflow	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:langflow:langflow:*:*~*~*~*~*~*~*	-
Langflow Inclusion of Functionality from Untrusted Control Sphere Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-829	T1595: Active Scanning, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://docs.langflow.org/1.9.0/release-notes

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-27137		router/upnp/src/ssdp.c in DD-WRT before 45724	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dd-wrt:dd-wrt:*:*:*:*:*:*	COXMO
DD-WRT Stack-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1587: Develop Capabilities, T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services	https://svn.dd-wrt.com/changeset/45724

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-58644</u>		Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*	-
Microsoft SharePoint Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1606: Forge Web Credentials	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58644

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-25089		Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox 4.2 all versions, FortiSandbox Cloud 5.0.4 through 5.0.5, FortiSandbox PaaS 5.0.4 through 5.0.5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:fortisandbox:*.~*~*~*~*~*~*	-
Fortinet FortiSandbox OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1588: Obtain Capabilities, T1059: Command and Scripting Interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-26-141

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-39808		Fortinet FortiSandbox 4.4.0 through 4.4.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:fortisandbox:*.~*~*~*~*~*~*	-
Fortinet FortiSandbox OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1083: File and Directory Discovery	https://fortiguard.fortinet.com/psirt/FG-IR-26-100

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-46817		Oracle Payments product 12.2.3-12.2.15	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:e-business_suite:*.~*~*~*~*~*~*	-
Oracle E-Business Suite Improper Privilege Management Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269, CWE-287, CWE-306	T1059: Command and Scripting Interpreter, T1083: File and Directory Discovery	https://www.oracle.com/security-alerts/cspumay2026.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4346		KNX devices that use KNX Connection Authorization and support Option 1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:knx:connection_authorization:-:*:*:*:*:*	-
KNX Association KNX Protocol Connection Authorization Option 1 Overly Restrictive Account Lockout Mechanism Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-645	T1133: External Remote Services, T0847: Replication Through Removable Media, T0809: Data Destruction	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-56155</u>		Windows 10, Windows Server 2012, 2016, 2019, 2022, 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:*:*:*:*:*:*:*:* *.*	-
Microsoft Active Directory Federation Services Insufficient Granularity of Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1220	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56155

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-56164</u>		Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint_server:*:*:*:subscription:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2016:*:*:*:enterprise:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*	-
Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56164

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-15409</u>		SonicWall SMA1000 Series 6210, 7210, 8200v 12.4.3-03245, 12.4.3-03387 and 12.4.3-03434 (platform-hotfix) 12.5.0-02283, 12.5.0-02624 and 12.5.0-02800 (platform-hotfix)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma6210_firmware:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma7210_firmware:*:*:*:*:*:* cpe:2.3:a:sonicwall:sma8200v:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-15410</u>		SonicWall SMA1000 Series 6210, 7210, 8200v 12.4.3-03245, 12.4.3-03387 and 12.4.3-03434 (platform-hotfix) 12.5.0-02283, 12.5.0-02624 and 12.5.0-02800 (platform-hotfix)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma6210_firmware:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma7210_firmware:*:*:*:*:*:* cpe:2.3:a:sonicwall:sma8200v:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2008-4128		Cisco IOS 12.4 on the 871 Integrated Services Router	Berserk Bear, Energetic Bear, Static Tundra
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:ios:12.4:*.~.*.*.*.*.*.*.*.*	-
Cisco IOS Cross-Site Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-352	T1059: Command and Scripting Interpreter, T1189: Drive-by Compromise	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-56291</u>		Balbooa Forms (`com_baforms`) for Joomla: all versions up to and including 2.4.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:cisco:871_integrated_services_router:-:~.*.*.*.*.*.*.*.*	-
Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-434	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.balbooa.com/help/joomla-forms-documentation/basics/changelog , https://www.balbooa.com/joomla-forms

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-48939		iCagenda	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:joomlic:icagenda:*:*:*:*:*:joomla\!:*:*	-
iCagenda Unrestricted Upload of File with Dangerous Type Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-434	T1595: Active Scanning, T1588: Obtain Capabilities, T1505: Server Software Component	https://www.icagenda.com/docs/changelog/icagenda-3-9-15 , https://www.icagenda.com/docs/changelog/icagenda-4-0-8

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-48908		SP Page Builder for Joomla	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ollyo:sp_page_builder:*:*:*:*:*:joomla\!:*:*	ChocoPoC RAT
JoomShaper SP Page Builder Unrestricted Upload of File with Dangerous Type Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1505: Server Software Component, T1059: Command and Scripting Interpreter, T1027: Obfuscated Files	https://extensions.joomla.org/extension/sp-page-builder/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-55255		Langflow Prior to 1.9.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:langflow:langflow:*:*:*:*:*:*	-
Langflow Authorization Bypass Through User-Controlled Key Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-639	T1078: Valid Accounts, T1068: Exploitation for Privilege Escalation, T1552: Unsecured Credentials	https://github.com/langflow-ai/langflow/commit/2c9f498d664a3c32698b57d7c5e752625291060e

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-56290		Page Builder CK a Joomla extension by joomlack.fr, all versions < 3.6.0.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:joomlack:page_builder_ck:*:*:*:*:*:joomla\!:*.*	-
Joomlack Page Builder Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1588: Obtain Capabilities, T1505: Server Software Component, T1036: Masquerading	https://forum.joomlack.fr/index.php/page-builder-ck/21627-nouvelle-version-de-pbck-et-joomla-3

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-48282</u>		ColdFusion versions 2025.9, 2023.20 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:coldfusion:*:*:*:*:*:*	-
Adobe ColdFusion Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-45659</u>		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:2019:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2016:*:*:*:*:enterprise:*:* cpe:2.3:a:microsoft:sharepoint_server:-:*:*:*:subscription:*:*	-
Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application,T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45659

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

August 04, 2026 • 06:30 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com