Date of Publication
December 1, 2025

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

November 2025

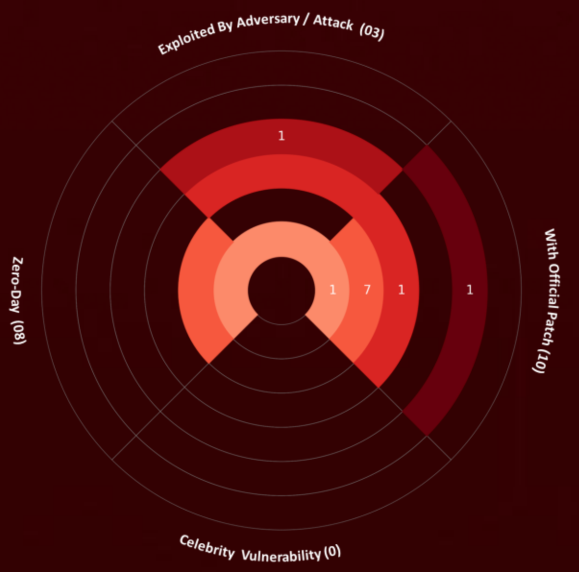
Table of Contents

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 November 2025, **11** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **eight** are **zero-day** vulnerabilities; **three** have been **exploited** by known threat actors and employed in attacks.

11
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2021-26829	OpenPLC ScadaBR Cross-site Scripting Vulnerability	OpenPLC ScadaBR	5.4	✗	✗	December 19, 2025
CVE-2025-61757	Oracle Fusion Middleware Missing Authentication for Critical Function Vulnerability	Oracle Fusion Middleware	9.8	✓	✓	December 12, 2025
CVE-2025-13223	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8	8.8	✓	✓	December 10, 2025
CVE-2025-58034	Fortinet FortiWeb OS Command Injection Vulnerability	Fortinet FortiWeb	7.2	✓	✓	November 25, 2025
CVE-2025-64446	Fortinet FortiWeb Path Traversal Vulnerability	Fortinet FortiWeb	9.8	✓	✓	November 21, 2025
CVE-2025-12480	Gladinet Triofox Improper Access Control Vulnerability	Gladinet Triofox	9.1	✗	✓	December 3, 2025
CVE-2025-62215	Microsoft Windows Race Condition Vulnerability	Microsoft Windows	7.0	✓	✓	December 3, 2025
CVE-2025-9242	WatchGuard Firebox Out-of-Bounds Write Vulnerability	WatchGuard Firebox	9.8	✗	✓	December 3, 2025
CVE-2025-21042	Samsung Mobile Devices Out-of-Bounds Write Vulnerability	Samsung Mobile Devices	8.8	✓	✓	December 1, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2025-48703	CWP Control Web Panel OS Command Injection Vulnerability	CWP Control Web Panel	9.0	✓	✓	November 25, 2025
CVE-2025-11371	Gladinet CentreStack and Triofox Files or Directories Accessible to External Parties Vulnerability	Gladinet CentreStack and Triofox	7.5	✓	✓	November 25, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26829	✗	OpenPLC ScadaBR through 0.9.1 on Linux and through 1.12.4 on Windows	TwoNet
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:openplcproject:scadabr:*:*:*:*:*:linux:*:* cpe:2.3:a:openplcproject:scadabr:*:*:*:*:*:windows:*:*	-
OpenPLC ScadaBR Cross-site Scripting Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1078: Valid Accounts, T1083: File and Directory Discovery, T1059: Command and Scripting Interpreter	✗

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-61757	✗	Oracle Fusion Middleware Version 12.2.1.4.0 and 14.1.2.1.0	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:identity_manager:12.2.1.4.0:*:*:*:*:*:*:* cpe:2.3:a:oracle:identity_manager:14.1.2.1.0:*:*:*:*:*:*:*	-
Oracle Fusion Middleware Missing Authentication for Critical Function Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059: Command and Scripting Interpreter	https://support.oracle.com/rs?type=doc&id=3105435.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-13223	✗	Google Chrome prior to 142.0.7444.175	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
	✗		
Google Chromium V8 Type Confusion Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1189: Drive-by Compromise, T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_17.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-58034	✗	FortiWeb 8.0 - 8.0.0 through 8.0.1 FortiWeb 7.6 - 7.6.0 through 7.6.5 FortiWeb 7.4 - 7.4.0 through 7.4.10 FortiWeb 7.2 - 7.2.0 through 7.2.11 FortiWeb 7.0 - 7.0.0 through 7.0.11	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*	-
	✓		
Fortinet FortiWeb OS Command Injection Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://fortiguard.fortinet.com/psirt/FG-IR-25-513

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-64446	✗	Fortinet FortiWeb 8.0 - 8.0.0 through 8.0.1 Fortinet FortiWeb 7.6 - 7.6.0 through 7.6.4 Fortinet FortiWeb 7.4 - 7.4.0 through 7.4.9 Fortinet FortiWeb 7.2 - 7.2.0 through 7.2.11 Fortinet FortiWeb 7.0 - 7.0.0 through 7.0.11	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*	-
Fortinet FortiWeb Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-23	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-25-910

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-12480	✗	Gladinet Triofox version 16.4.10317.56372	UNC6485
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gladinet:triofox:*:*:*:*:*:*:*:*	-
Gladinet Triofox Improper Access Control Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://access.triofox.com/releases_history/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-62215	✗	Windows: 10 - 11 25H2 Windows Server: 2019 - 2025	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_serve:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
Microsoft Windows Race Condition Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-362	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-62215

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-9242	✗	Fireware OS 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and including 12.11.3 and 2025.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:watchguard:fireware:*:*:*:*:*:*:*:* cpe:2.3:h:watchguard:firebox:*:*:*:*:*:*:*:*	-
WatchGuard Firebox Out-of-Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://software.watchguard.com/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21042	✗	Android 13, 14, 15	CL-UNK-1054
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:samsung:android:*:*:*:*:*:*	LANDFALL
Samsung Mobile Devices Out-of-Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter	https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=04

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48703	✗	CWP (aka Control Web Panel or CentOS Web Panel) before 0.9.8.1205	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:control-webpanel:webpanel:*:*:*:*:*:*:*:*	-
CWP Control Web Panel OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://control-webpanel.com/changelog

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-11371	✗	Gladinet CentreStack and Triofox: All versions prior to and including 16.7.10368.56560	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gladinet:centrestack:*:*:*:*:*:*:*:* cpe:2.3:a:gladinet:triofox:*:*:*:*:*:*:*:*	-
Gladinet CentreStack and Triofox Files or Directories Accessible to External Parties Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-552	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://www.centrestack.com/p/gce_latest_release.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 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.

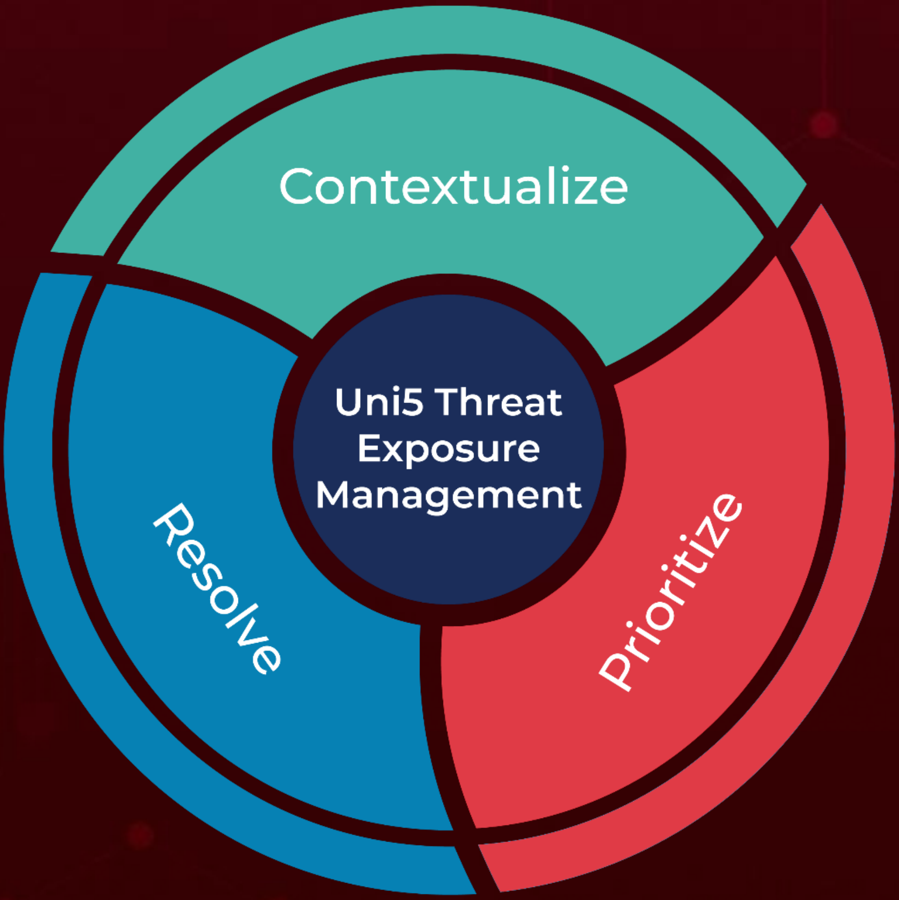
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

December 1, 2025 • 9:30 AM

More at www.hivepro.com