Date of Publication
June 3, 2025

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

May 2025

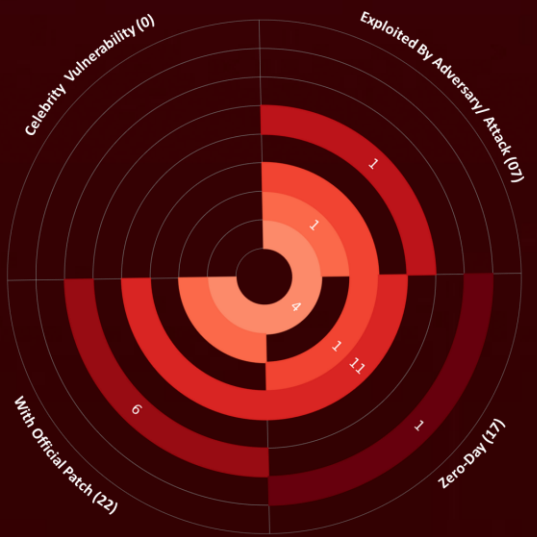
Table of Contents

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 May 2025, **twenty five** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **seventeen** are **zero-day** vulnerabilities; **seven** have been **exploited** by known threat actors and employed in attacks.

25
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-4632	Samsung MagicINFO 9 Server Path Traversal Vulnerability	Samsung MagicINFO 9 Server	9.8	✓	✓	June 12, 2025
CVE-2023-38950	ZKTeco BioTime Path Traversal Vulnerability	ZKTeco BioTime	7.5	✗	✓	June 9, 2025
CVE-2024-27443	Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	6.1	✗	✓	June 9, 2025
CVE-2025-27920	Srimax Output Messenger Directory Traversal Vulnerability	Srimax Output Messenger	7.2	✓	✓	June 9, 2025
CVE-2024-11182	MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability	MDaemon Email Server	5.3	✓	✓	June 9, 2025
CVE-2025-4428	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	8.8	✓	✓	June 9, 2025
CVE-2025-4427	Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	7.5	✓	✓	June 9, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-42999	SAP NetWeaver Deserialization Vulnerability	SAP NetWeaver	9.1	✓	✓	June 5, 2025
CVE-2024-12987	DrayTek Vigor Routers OS Command Injection Vulnerability	DrayTek Vigor Routers	6.9	✓	✓	June 5, 2025
CVE-2025-4664	Google Chromium Loader Insufficient Policy Enforcement Vulnerability	Google Chromium	4.3	✓	✓	June 5, 2025
CVE-2025-32756	Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability	Fortinet Multiple Products	9.8	✓	✓	June 4, 2025
CVE-2025-32709	Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability	Microsoft Windows	7.8	✓	✓	June 3, 2025
CVE-2025-30397	Microsoft Windows Scripting Engine Type Confusion Vulnerability	Microsoft Windows	7.5	✓	✓	June 3, 2025
CVE-2025-32706	Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability	Microsoft Windows	7.8	✓	✓	June 3, 2025
CVE-2025-32701	Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability	Microsoft Windows	7.8	✓	✓	June 3, 2025
CVE-2025-30400	Microsoft Windows DWM Core Library Use-After-Free Vulnerability	Microsoft Windows	7.8	✓	✓	June 3, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-47729	TeleMessage TM SGNL Hidden Functionality Vulnerability	TeleMessage TM SGNL	4.9	✗	✗	June 2, 2025
CVE-2024-11120	GeoVision Devices OS Command Injection Vulnerability	GeoVision Multiple Devices	9.8	✓	✗	May 28, 2025
CVE-2024-6047	GeoVision Devices OS Command Injection Vulnerability	GeoVision Multiple Devices	9.8	✗	✗	May 28, 2025
CVE-2025-27363	FreeType Out-of-Bounds Write Vulnerability	FreeType FreeType	8.1	✗	✓	May 27, 2025
CVE-2025-3248	Langflow Missing Authentication Vulnerability	Langflow Langflow	9.8	✗	✓	May 26, 2025
CVE-2025-34028	Commvault Command Center Path Traversal Vulnerability	Commvault Command Center	10.0	✗	✓	May 23, 2025
CVE-2024-58136	Yiiframework Yii Improper Protection of Alternate Path Vulnerability	Yiiframework Yii	9.8	✓	✓	May 23, 2025
CVE-2024-38475	Apache HTTP Server Improper Escaping of Output Vulnerability	Apache HTTP Server	9.1	✗	✓	May 22, 2025
CVE-2023-44221	SonicWall SMA100 Appliances OS Command Injection Vulnerability	SonicWall SMA100 Appliances	7.2	✗	✓	May 22, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4632	✗	Samsung MagicInfo 9 Server Versions prior to 21.1052	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:samsung:magicinfo_9_server:*:*:*:*:*:*:*:*	-
Samsung MagicINFO 9 Server Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://eu.community.samsung.com/t5/samsung-solutions/update-magicinfo-server-v9-21-1052-0-setup-file/ta-p/11374265

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38950	✗	ZKTeco BioTime version 8.5.5	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:zkteco:biotime:8.5.5:*:*:*:*:*:*:*	-
ZKTeco BioTime Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://www.zkteco.me/download; https://www.zkteco.me/product-details/biotime-95

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27443	✗	Synacor Zimbra Collaboration Suite (ZCS) 9.0 and 10.0.	APT28
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:zimbra:collaboration:-:*:*:*:*:*:*:*	SpyPress
Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059.007: Command and Scripting Interpreter: JavaScript; T1566: Phishing; T1190: Exploit Public-Facing Application	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.7#Security_Fixes

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-27920	✗	Output Messenger before 2.0.63	Marbled Dust
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:output_messenger:out_put_messenger:-:*:*:*:*:*:*:*	-
Srimax Output Messenger Directory Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://www.outputmessenger.com/cve-2025-27920/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-11182	✗	MDaemon Email Server before version 24.5.1c	APT28
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:mdaemon:mdaemon:*:*:*:*:*:*:*:*	SpyPress
MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1204: User Execution	https://files.mdaemon.com/mdaemon/beta/RelNotes_en.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4428	✗	Ivanti Endpoint Manager Mobile: 11.12.0.4 and prior, 12.3.0.1 and prior, 12.4.0.1 and prior, 12.5.0.0 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4427	✗	Ivanti Endpoint Manager Mobile: 11.12.0.4 and prior, 12.3.0.1 and prior, 12.4.0.1 and prior, 12.5.0.0 and prior	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-42999	✗	SAP NetWeaver Version 7.50	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sap:netweaver:*:*:*:*:*:*:*:*	RansomEXX
SAP NetWeaver Deserialization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1505.003: Server Software Component: Web Shell	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-12987	✗	DrayTek Vigor2960 and Vigor300B 1.5.1.4.	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:draytek:vigor300b:-:*:*:*:*:*:*:* cpe:2.3:h:draytek:vigor2960:-:*:*:*:*:*:*:*	-
DrayTek Vigor Routers OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77 CWE-78	T1059: Command and Scripting Interpreter; T1202: Indirect Command Execution	https://www.draytek.com/support/resources/routers

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4664	✗	Google Chrome V8 prior to 136.0.7103.113 Microsoft Edge Version prior to 136.0.3240.76	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Google Chromium Loader Insufficient Policy Enforcement Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-346	T1528: Steal Application Access Token; T1189 : Drive-by Compromise; T1204: User Execution	https://www.google.com/intl/en/chrome/?standalone=1

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="4">CVE-2025-32756</td><td>✗</td><td rowspan="2">FortiCamera Version 2.1.0 through 2.1.3
FortiCamera 2.0 All Versions
FortiCamera 1.1 All Versions
FortiMail Version 7.6.0 through 7.6.2
FortiMail Version 7.4.0 through 7.4.4
FortiMail Version 7.2.0 through 7.2.7
FortiMail Version 7.0.0 through 7.0.8
FortiNDR Version 7.6.0
FortiNDR Version 7.4.0 through 7.4.7
FortiNDR Version 7.2.0 through 7.2.4
FortiNDR 7.1 All Versions
FortiNDR Version 7.0.0 through 7.0.6
FortiNDR 1.1 – 1.5 All Versions
FortiRecorder Version 7.2.0 through 7.2.3
FortiRecorder Version 7.0.0 through 7.0.5
FortiRecorder Version 6.4.0 through 6.4.5
FortiVoice Version 7.2.0
FortiVoice Version 7.0.0 through 7.0.6
FortiVoice Version 6.4.0 through 6.4.10</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:fortinet:fortivoice:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortirecorder:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortindr:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:fortimail:*:*:*:*:*:*:*:*
cpe:2.3:a:fortinet:forticamera:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability</td><td>✓</td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-121</td><td>T1059: Command and Scripting Interpreter;
T1068: Exploitation for Privilege Escalation;
T1053.003: Scheduled Task/Job: Cron</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-25-254</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32709		Windows: 10 21H2 - 11 24H2 Windows Server: 2012 - 2025	-
	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 Ancillary Function Driver for WinSock Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32709

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32701		Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	-
	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 Common Log File System (CLFS) Driver Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32701

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32706		Windows: 10 21H2 - 11 24H2 Windows Server: 2008 - 2025	-
	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 Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-32706

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30397	✗	Windows: 10 - 11 Windows Server: 2008 - 2025 Microsoft Internet Explorer: 11	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:microsoft_internet_explorer:-:*:*:*:*:*:*:*	-
Microsoft Windows Scripting Engine Type Confusion Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059: Command and Scripting Interpreter; T1204.001: User Execution: Malicious Link; T1566: Phishing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30397

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30400	✗	Windows: 10 21H2 - 11 24H2 Windows Server: 2012 Gold - 2025	-
	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 DWM Core Library Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-30400

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-47729	✗	TeleMessage Text Message Archiver (TM SGNL/Archive Signal) versions up to 2025-05-05	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:telemessage:text_message_archiver:*:*:*:*:*:*:*:*	-
TeleMessage TM SGNL Hidden Functionality Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-912	T1005: Data from Local System	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-27363	✗	FreeType (FreeType) Version form 0.0.0 through 2.13.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:freetype:freetype:*:*:*:*:*:*:*:*	-
FreeType Out-of-Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://freetype.org/download.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-2024-11120</td><td>✗</td><td rowspan="2">GeoVision VS12
GeoVision VS11
GeoVision
DSP_LPR_V3
GeoVision LX 4 V2
GeoVision LX 4 V3</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:geovision:gvlx_4_v3_firmware:*:*:*:*:*:*:*:*
cpe:2.3:o:geovision:gvlx_4_v2_firmware:*:*:*:*:*:*:*:*
cpe:2.3:o:geovision:gv-vs12_firmware:*:*:*:*:*:*:*:*
cpe:2.3:o:geovision:gv-vs11_firmware:*:*:*:*:*:*:*:*
cpe:2.3:o:geovision:gv-dsp_lpr_v3_firmware:*:*:*:*:*:*:*:*</td><td rowspan="2">Mirai, LZRD</td></tr>
<tr><td>GeoVision Devices OS Command Injection Vulnerability</td><td>✗</td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-78</td><td>T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application</td><td>-</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-6047	✗	GeoVision VS12 GeoVision VS11 GeoVision DSP_LPR_V3 GeoVision LX 4 V2 GeoVision LX 4 V3	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:geovision:gvlx_4_v3_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gvlx_4_v2_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs12_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs11_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-dsp_lpr_v3_firmware:*:*:*:*:*:*:*:*	Mirai, LZRD
GeoVision Devices OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-3248	✗	Langflow versions prior to 1.3.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:langflow-ai:langflow:*:*:*:*:*:*:*:*	-
Langflow Missing Authentication Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1059.006: Python	https://github.com/langflow-ai/langflow/releases/tag/1.3.0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-34028	✗	Commvault Command Center versions before 11.38.20	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:commvault:commvault:*:*:*:*:*:*:*:*	-
Commvault Command Center Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306 CWE-22	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1203: Exploitation for Client Execution	https://documentation.commvault.com/v11/essential/installing_commvault_software_updates_on_demand.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-58136	✗	Yiiframework Yii	Mimo (aka Hezb)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:yiiframework:yii:*:*:*:*:*:*:*:*	XMRig
Yiiframework Yii Improper Protection of Alternate Path Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-424	T1068: Exploitation for Privilege Escalation	https://github.com/yiisoft/yii2/pull/20232

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38475	✗	SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:sonicwall:sma_firmware:*:*:*:*:*:*:*:*	-
Apache HTTP Server Improper Escaping of Output Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-116	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://httpd.apache.org/download.cgi

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-44221</td><td>  </td><td rowspan="3">SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions</td><td rowspan="3">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td></tr>
<tr><th>NAME</th><th>BAS ATTACKS</th><th>AFFECTED CPE</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th></tr>
<tr><td rowspan="3">SonicWall SMA100 Appliances OS Command Injection Vulnerability</td><td>  </td><td rowspan="2">cpe:2.3:o:sonicwall:sma_firmware:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><th>CWE ID</th><th>ASSOCIATED TTPs</th><th>PATCH LINK</th></tr>
<tr><td>CWE-78</td><td>T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter</td><td>https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018</td></tr>
</table>

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.

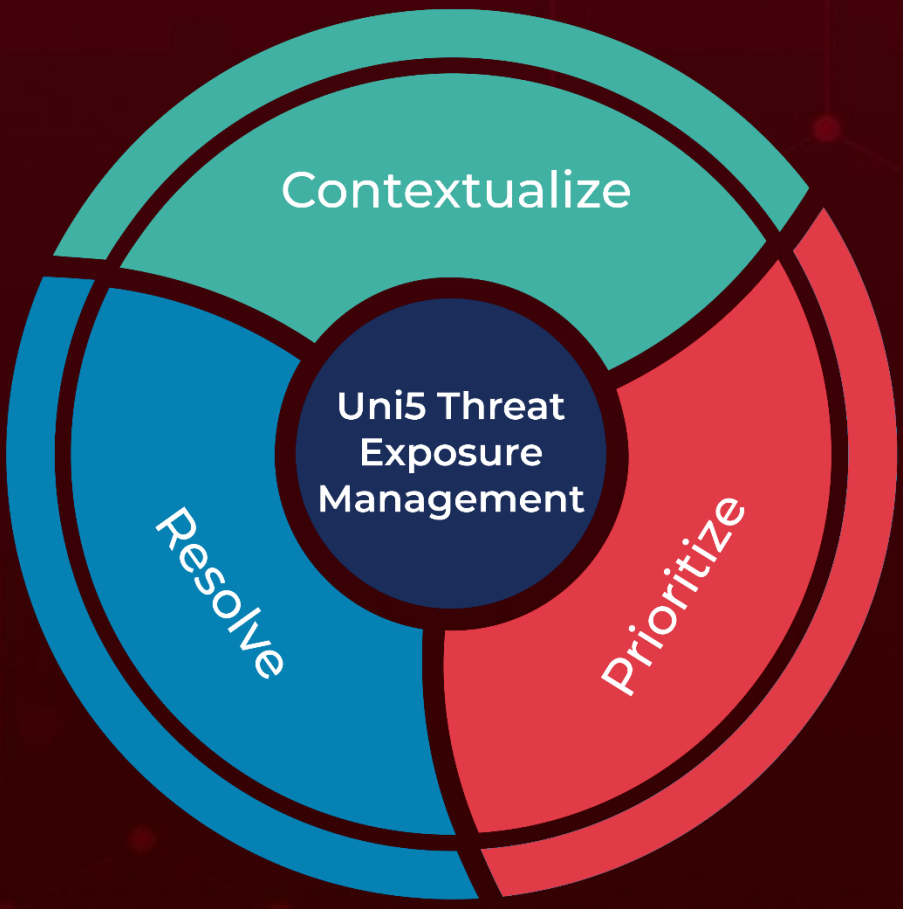
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

June 3, 2025 . 5:30 AM

More at www.hivepro.com