Date of Publication
January 2, 2026

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

December 2025

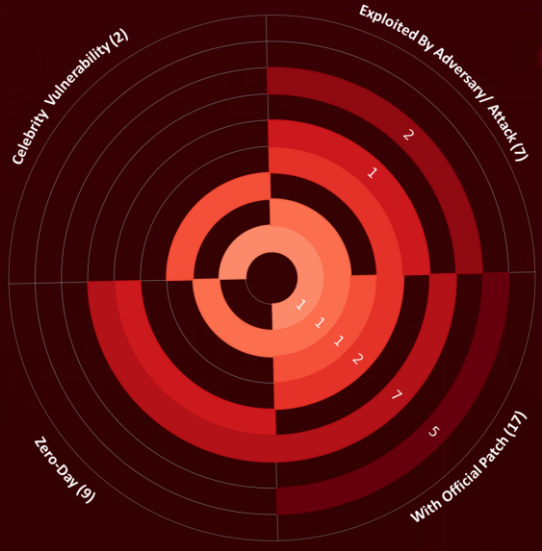
Table of Contents

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

20
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-14847	MongoBleed (MongoDB and MongoDB Server Improper Handling of Length Parameter Inconsistency Vulnerability)	MongoDB and MongoDB Server	7.5	✗	✓	January 19, 2026
CVE-2023-52163	Digiever DS-2105 Pro Missing Authorization Vulnerability	Digiever DS-2105 Pro	8.8	✗	✗	January 12, 2026
CVE-2025-14733	WatchGuard Firebox Out of Bounds Write Vulnerability	WatchGuard Firebox	9.8	✓	✓	December 26, 2025
CVE-2025-59374	ASUS Live Update Embedded Malicious Code Vulnerability	ASUS Live Update	9.8	✗	✓	January 7, 2026
CVE-2025-40602	SonicWall SMA1000 Missing Authorization Vulnerability	SonicWall SMA1000 appliance	6.6	✓	✓	December 24, 2025
CVE-2025-20393	Cisco Multiple Products Improper Input Validation Vulnerability	Cisco Multiple Products	10	✓	✗	December 24, 2025
CVE-2025-59718	Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability	Fortinet Multiple Products	9.8	✗	✓	December 23, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-14611	Gladinet CentreStack and Triofox Hard Coded Cryptographic Vulnerability	Gladinet CentreStack and Triofox	9.8	✓	✓	January 5, 2026
CVE-2025-43529	Apple Multiple Products Use-After-Free WebKit Vulnerability	Apple Multiple Products	8.8	✓	✓	January 5, 2026
CVE-2018-4063	Sierra Wireless AirLink ALEOS Unrestricted Upload of File with Dangerous Type Vulnerability	Sierra Wireless AirLink ALEOS	8.8	✗	✓	January 2, 2026
CVE-2025-14174	Google Chromium Out of Bounds Memory Access Vulnerability	Google Chromium	8.8	✓	✓	January 2, 2026
CVE-2025-58360	OSGeo GeoServer Improper Restriction of XML External Entity Reference Vulnerability	OSGeo GeoServer	9.8	✗	✓	January 1, 2026
CVE-2025-6218	RARLAB WinRAR Path Traversal Vulnerability	RARLAB WinRAR	7.8	✗	✓	December 30, 2025
CVE-2025-62221	Microsoft Windows Use After Free Vulnerability	Microsoft Windows	7.8	✓	✓	December 30, 2025
CVE-2022-37055	D-Link Routers Buffer Overflow Vulnerability	D-Link Routers	9.8	✗	✗	December 29, 2025
CVE-2025-66644	Array Networks ArrayOS AG OS Command Injection Vulnerability	Array Networks ArrayOS AG	9.8	✗	✓	December 29, 2025
CVE-2025-55182	React2Shell (Meta React Server Components Remote Code Execution Vulnerability)	Meta React Server Components	10	✗	✓	December 12, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2021-26828	OpenPLC ScadaBR Unrestricted Upload of File with Dangerous Type Vulnerability	OpenPLC ScadaBR	8.8	✗	✓	December 24, 2025
CVE-2025-48633	Android Framework Information Disclosure Vulnerability	Android Framework	5.5	✓	✓	December 23, 2025
CVE-2025-48572	Android Framework Privilege Escalation Vulnerability	Android Framework	7.8	✓	✓	December 23, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-14847	MongoBleed	MongoDB 8.2.0 through 8.2.2 MongoDB 8.0.0 through 8.0.16 MongoDB 7.0.0 through 7.0.27 MongoDB 6.0.0 through 6.0.26 MongoDB 5.0.0 through 5.0.31 MongoDB 4.4.0 through 4.4.29 All MongoDB Server v4.2 versions All MongoDB Server v4.0 versions All MongoDB Server v3.6 versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:mongodb:mongodb:*:*:*:*:*:*:*:*	-
MongoDB and MongoDB Server Improper Handling of Length Parameter Inconsistency Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-130	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials, T1082: System Information Discovery	https://www.mongodb.com/try/download/community, https://www.mongodb.com/community/forums/t/important-mongodb-patch-available/332977

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-52163	✗	Digiever DS-2105 Pro 3.1.0.71-11 devices	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:digiever:ds-2105_pro:-:*:*:*:*:*:*:*	Mirai and ShadowV2
Digiever DS-2105 Pro Missing Authorization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	EOL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-14733	✗	WatchGuard Fireware OS 11.10.2 up to and including 11.12.4_Update1, 12.0 up to and including 12.11.5 and 2025.1 up to and including 2025.1.3	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:watchguard:fireware:*:*:*:*:*:*:*:*	-
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; T1499 : Endpoint Denial of Service	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-59374	✗	Asus Live Update before 3.6.6	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:asus:live_update:*:*:*:*:*:*:*:*	-
ASUS Live Update Embedded Malicious Code Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1195: Supply Chain Compromise, T1566: Phishing, T1059: Command and Scripting Interpreter	https://www.asus.com/us/support/faq/1018727/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-40602	✗	SonicWall SMA1000: 12.4.3-03093 (platform-hotfix) and earlier versions, 12.5.0-02002 (platform-hotfix) and earlier versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:sonicwall:sma_1000_firmware:*:*:*:*:*:*:*:*	-
SonicWall SMA1000 Missing Authorization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-862, CWE-250	T1078: Valid Accounts, T1068: Exploitation for Privilege Escalation	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-20393</td><td>  </td><td rowspan="2">Cisco Secure Email Gateway (SEG) and Cisco Secure Email and Web Manager (SEWM): All Cisco AsyncOS versions (physical and virtual appliances)</td><td rowspan="2">UAT-9686</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:cisco:secure_email_and_web_manager_virtual_appliance:-:*:*:*:*:*:*:*
cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance:-:*:*:*:*:*:*:*
cpe:2.3:h:cisco:secure_email_and_web_manager:-:*:*:*:*:*:*:*
cpe:2.3:h:cisco:secure_email_gateway:-:*:*:*:*:*:*:*</td><td rowspan="2">AquaShell, AquaTunnel, AquaPurge, and Chisel</td></tr>
<tr><td rowspan="3">Cisco Multiple Products Improper Input Validation Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-20</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>  </td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-59718	✗	Fortinet Fortios Before 7.0.18, Before 7.2.12, Before 7.4.9, Before 7.6.4; Fortinet Fortiproxy Before 7.0.22, Before 7.2.15, Before 7.4.11, Before 7.6.4; Fortinet Fortiswitchmanager Before 7.0.6, Before 7.2.7	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS Attacks**	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiswitchmanager:*:*:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	-
Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-347	T1190: Exploit Public-Facing Application, T1071: Application Layer Protocol, T1556: Modify Authentication Process	https://www.fortiguard.com/psirt/FG-IR-25-647

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-14611	✗	Gladinet CentreStack and Triofox prior to version 16.12.10420.56791	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:gladinet:centrestack:*:*:*:*:*:*:*:*:* cpe:2.3:a:gladinet:triofox:*:*:*:*:*:*:*:*:*	Cl0p
Gladinet CentreStack and Triofox Hard Coded Cryptographic Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINKS**
	CWE-798	T1552: Unsecured Credentials, T1068: Exploitation for Privilege Escalation	https://www.centrestack.com/p/gce_latest_release.html, https://access.triofox.com/releases_history/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-43529	✗	iOS / iPadOS: versions earlier than 26.2 and 18.7.3, macOS: versions earlier than Tahoe 26.2, Safari: versions earlier than 26.2, tvOS: versions earlier than 26.2, watchOS: versions earlier than 26.2, visionOS: versions earlier than 26.2, Google Chrome (macOS): versions earlier than 143.0.7499.110, Microsoft Edge (macOS): versions prior to 143.0.3650.80	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS Attacks**	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* 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:*:*:*:*:*:*:*:* cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Apple Multiple Products Use-After-Free WebKit Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-416	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/100100 , https://support.apple.com/en-us/125892 , https://support.apple.com/en-us/125886 , https://support.apple.com/en-us/125885 , https://support.apple.com/en-us/125884 , https://support.apple.com/en-us/125892 , https://support.apple.com/en-us/125889 , https://support.apple.com/en-us/125890 , https://support.apple.com/en-us/125891 , https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_10.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-2018-4063</td><td>✗</td><td rowspan="2">Sierra Wireless AirLink ES450 firmware version 4.9.3</td><td rowspan="2">Chaya_005</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:sierrawireless:aleos:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Sierra Wireless AirLink ALEOS Unrestricted Upload of File with Dangerous Type Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-502</td><td>T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution</td><td>https://source.sierrawireless.com/resources/airlink/software_reference_docs/release-notes/aleos/?#sthash.0GsJeF34.dpbs</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-14174</td><td>✗</td><td rowspan="2">Google Chrome prior 143.0.7499.109 (Linux), BEFORE 143.0.7499.109/.110 (Windows/Mac), iOS / iPadOS: versions earlier than 26.2 and 18.7.3, macOS: versions earlier than Tahoe 26.2, Safari: versions earlier than 26.2, tvOS: versions earlier than 26.2, watchOS: versions earlier than 26.2, visionOS: versions earlier than 26.2, Google Chrome (macOS): versions earlier than 143.0.7499.110, Microsoft Edge (macOS): versions prior to 143.0.3650.80</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:google:chrome:*:*:*:*:*:*:*:*
cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*
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:*:*:*:*:*:*:*:*
cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Google Chromium Out of Bounds Memory Access Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-122</td><td>T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter</td><td>https://www.google.com/intl/en/chrome/?standalone=1 , https://support.apple.com/en-us/100100</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-58360	✗	GeoServer version 2.26.0 to before 2.26.2 and before 2.25.6,	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:geoserver:geoserver:*:*:*:*:*:*:*:*	-
OSGeo GeoServer Improper Restriction of XML External Entity Reference Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1190: Exploit Public-Facing Application	https://github.com/geoserver/geoserver/security/advisories/GHSA-fjf5-xgmq-5525

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-6218	✗	WinRAR Version Prior to 7.12	Gamaredon, APT-C-08
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:rarlab:winrar:*:*:*:*:*	Pteranodon, GamaWiper
RARLAB WinRAR Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	https://www.win-rar.com/download.html?&L=0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-62221	✗	Windows Server 2022, 2025; Windows 11 Version 25H2; Windows 10 Version 1809	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	-
Microsoft Windows Use After Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-62221

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-37055	✗	D-Link Go-RT-AC750 GORTAC750_revA_v101b03 and GO-RT-AC750_revB_FWv200b02	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:dlink:go-rt-ac750:revision_b:*:*:*:*:*:*:*:* cpe:2.3:o:dlink:go-rt-ac750_firmware:2.00b02:*:*:*:*:*:*:*	ShadowV2
D-Link Routers Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1068: Exploitation for Privilege Escalation	EOL

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-66644</td><td>  </td><td rowspan="2">Array Networks ArrayOS AG before 9.4.5.9</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:arraynetworks:arrayos_ag:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Array Networks ArrayOS AG OS Command Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-78</td><td>T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter</td><td>https://support.arraynetworks.net/</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-55182</td><td>React2Shell</td><td rowspan="2">react-server-dom-webpack, react-server-dom-parcel, react-server-dom-turbopack versions: 19.0.0, 19.1.0, 19.1.1, 19.2.0
Next.js versions: 14.3.0-canary.77+, 15.x, 16.x (before 16.0.7)
React Router, Waku, RedwoodSDK, @parcel/rsc, @vitejs/plugin-rsc</td><td rowspan="2">Earth Lamia (aka UNC5454), Jackpot Panda and UNC5174 (aka Uteus, CL-STA-1015), UNC6600, UNC6588, UNC6603, UNC6595, UNC5342</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:facebook:react:*:*:*:*:*:*:*:*
cpe:2.3:a:vercel:next.js:*:*:*:*:*:node.js:*:*
cpe:2.3:a:remix:react_router:*:*:*</td><td rowspan="2">XMRig, Sliver, PeerBlight, EtherRAT, Snowlight, Vshell, Noodle RAT (aka ANGRYREBEL.LINUX), KSwapDoor, Auto-color, Minocat, Compood, and Hisonic</td></tr>
<tr><td rowspan="2">Meta React Server Components Remote Code Execution Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-502</td><td>T1190: Exploit Public-Facing Application, T1059.007: JavaScript, T1059: Command and Scripting Interpreter</td><td>https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26828	✗	OpenPLC ScadaBR through 0.9.1 on Linux and through 1.12.4 on Windows	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:scadabr:scadabr:*:*:*:*:*:*:*:*	-
OpenPLC ScadaBR Unrestricted Upload of File with Dangerous Type Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://github.com/SCADA-LTS/Scada-LTS/pull/2174, https://github.com/SCADA-LTS/Scada-LTS/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48633	✗	Android Framework	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:*:*:*:*:*:*:*:*	-
Android Framework Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1417: Input Capture, T1005: Data from Local System, T1068: Exploitation for Privilege Escalation	https://source.android.com/security/bulletin/2025-12-01

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48572		Android Framework	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:*:*:*:*:*:*:*:*	-
Android Framework Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1068: Exploitation for Privilege Escalation	https://source.android.com/security/bulletin/2025-12-01

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.

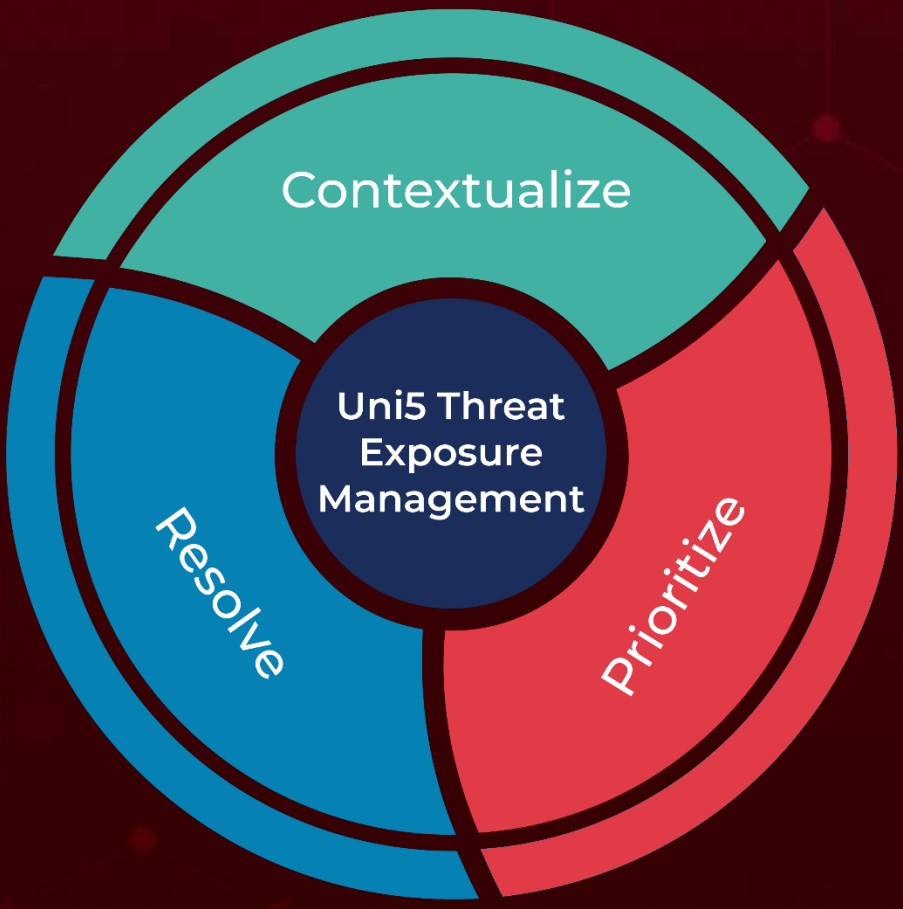
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

January 2, 2026 . 7:45 AM

More at www.hivepro.com