Date of Publication
October 1, 2025

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

September 2025

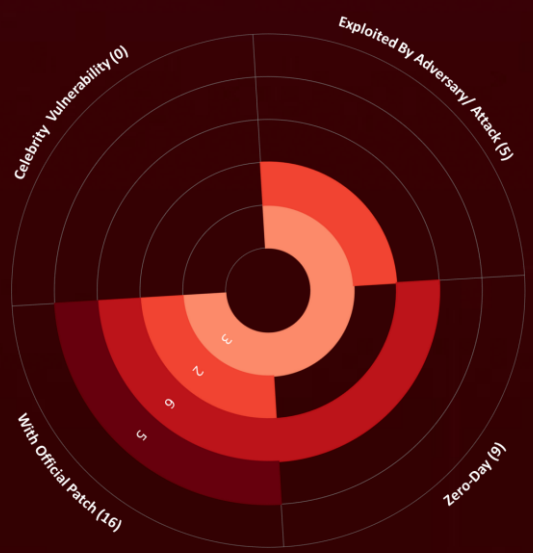
Table of Contents

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

16
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-32463	Sudo Inclusion of Functionality from Untrusted Control Sphere Vulnerability	Sudo	7.8	✗	✓	October 20, 2025
CVE-2025-59689	Libraesva Email Security Gateway Command Injection Vulnerability	Libraesva Email Security Gateway	6.1	✓	✓	October 20, 2025
CVE-2025-10035	Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability	Fortra GoAnywhere MFT	10	✓	✓	October 20, 2025
CVE-2025-20352	Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability	Cisco IOS and IOS XE	7.7	✓	✓	October 20, 2025
CVE-2021-21311	Adminer Server-Side Request Forgery Vulnerability	Adminer Adminer	7.2	✗	✓	October 20, 2025
CVE-2025-20362	Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense	6.5	✓	✓	September 26, 2025
CVE-2020-24363	TP-link TL-WA855RE Missing Authentication for Critical Function Vulnerability	TP-Link TL-WA855RE	8.8	✗	✓	September 23, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-20333	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense	9.9	✓	✓	September 26, 2025
CVE-2025-10585	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8	9.8	✓	✓	October 14, 2025
CVE-2025-5086	Dassault SystÃ¨mes DELMIA Apriso Deserialization of Untrusted Data Vulnerability	Dassault SystÃ¨mes DELMIA Apriso	9	✗	✓	October 2, 2025
CVE-2025-38352	Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability	Linux Kernel	7.4	✓	✓	September 25, 2025
CVE-2025-48543	Android Runtime Use-After-Free Vulnerability	Android Runtime	8.8	✓	✓	September 25, 2025
CVE-2025-53690	Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability	Sitecore Multiple Products	9	✓	✓	September 25, 2025
CVE-2023-50224	TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability	TP-Link TL-WR841N	6.5	✗	✓	September 24, 2025
CVE-2025-9377	TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability	TP-Link Multiple Routers	7.2	✗	✓	September 24, 2025
CVE-2025-55177	Meta Platforms WhatsApp Incorrect Authorization Vulnerability	Meta Platforms WhatsApp	5.4	✗	✓	September 23, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-32463	✗	Sudo before 1.9.17p1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sudo_project:sudo:*:*:*:*:*:*:*:*	-
Sudo Inclusion of Functionality from Untrusted Control Sphere Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-829	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://www.sudo.ws/security/advisories/chroot_bug/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-59689	✗	Libraesva ESG version 4.5, 5.0, 5.1, 5.2, 5.3, 5.4	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:libraesva:email_security_gateway:*:*:*:*:*:*:*:*	-
Libraesva Email Security Gateway Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://docs.libraesva.com/knowledgebase/security-advisory-command-injection-vulnerability-cve-2025-59689/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-10035	✗	Fortra GoAnywhere MFT versions before: 7.8.4, 7.6.3	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortra:goanywhere_managed_file_transfer:*:*:*:*:*:*:*:*	-
Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter; T1078 : Valid Accounts; T1190: Exploit Public-Facing Application	https://www.fortra.com/security/advisories/product-security/fi-2025-012

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-20352	✗	Cisco IOS & IOS XE Software, Meraki MS390 Switches - Meraki CS 17 and earlier, Cisco Catalyst 9300 Series Switches - Meraki CS 17 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:ios:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*:*:*	-
Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application; T1499 : Endpoint Denial of Service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-21311	✗	Adminer versions before 4.7.9	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adminer:adminer:*:*:*:*:*:*:*:*	-
Adminer Server-Side Request Forgery Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1078 : Valid Accounts; T1190: Exploit Public-Facing Application; T1499 : Endpoint Denial of Service	https://github.com/vrana/adminer/commit/ccd2374b0b12bd547417bf0dacdf153826c83351

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-20362	✗	Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23 Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7	UAT4356 (aka Storm-1849)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*	RayInitiator bootkit, Line Viper loader
Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) 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	https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-20333	✗	Cisco ASA Software: 9.16, 9.17, 9.18, 9.19, 9.20, 9.22, 9.23 Cisco FTD Software: 7.0, 7.2, 7.4, 7.6, 7.7	UAT4356 (aka Storm-1849)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*	RayInitiator bootkit, Line Viper loader
Cisco Secure Firewall Adaptive Security (ASA) Appliance and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation; T1542.004 Pre-OS Boot: ROMMONkit	https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_continued_attacks

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-10585	✗	Google Chrome prior to 140.0.7339.185	-
	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	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-5086	✗	DELMIA Apriso from Release 2020 through Release 2025	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:3ds:delmia_apriso:*:*:*:*:*:*:*:*	-
Dassault Systèmes DELMIA Apriso Deserialization of Untrusted Data Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter; T1202: Indirect Command Execution	https://www.3ds.com/trust-center/security/security-advisories/cve-2025-5086

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-38352	✗	Linux Kernel	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-367	T1204: User Execution, T1068: Exploitation for Privilege Escalation	https://git.kernel.org/stable/c/2c72fe18cc5f9f1750f5bc148cf1c94c29e106ff

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48543	✗	Android Runtime	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:*:*:*:*:*:*:*:*	-
Android Runtime Use-After-Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution	https://source.android.com/docs/security/bulletin/2025-09-01; https://android.googlesource.com/platform/art/+/a5889a1a85117d0b168ff5bb9e0c123d2cd6409f

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-53690	✗	Sitecore Experience Manager (XM) and Experience Platform (XP) Through Version 9.0, Experience Commerce (XC), Managed Cloud, AD Version 1.4 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sitecore:experience_platform:*:*:*:*:*:*:*:* cpe:2.3:a:sitecore:experience_manager:*:*:*:*:*:*:*:* cpe:2.3:a:sitecore:experience_commerce:*:*:*:*:*:*:*:*	WEEPSTEEL, EARTHWORM, DWAGENT, SHARPHOUND
Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-502	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://support.sitecore.com/kb?id=kb_article_view&sysparm_article=KB1003865

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-50224</td><td>✗</td><td rowspan="2">TP-Link TL-WR841N routers</td><td rowspan="2">Storm-0940</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:tp-link:tl-wr841n_firmware:3.16.9:build_200409:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:tl-wr841n:12:*:*:*:*:*:*:*</td><td rowspan="2">Quad 7 (7777)</td></tr>
<tr><td rowspan="2">TP-Link TL-WR841N Authentication Bypass by Spoofing Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-290</td><td>T1190: Exploit Public-Facing</td><td>https://www.tp-link.com/en/support/download/tl-wr841n/v12/#Firmware</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-9377</td><td>✗</td><td rowspan="2">Archer C7(EU) V2: before 241108 and TL-WR841N/ND(MS) V9: before 241108</td><td rowspan="2">Storm-0940</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:tp-link:tl-wr841n_firmware:*:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:tl-wr841n:v9:*:*:*:*:*:*:*:*
cpe:2.3:o:tp-link:tl-wr841nd_firmware:*:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:tl-wr841nd:9:*:*:*:*:*:*:*
cpe:2.3:o:tp-link:archer_c7_firmware:*:*:*:*:*:*:*:*
cpe:2.3:h:tp-link:archer_c7:2.0:*:*:*:*:*:*:*</td><td rowspan="2">Quad 7 (7777)</td></tr>
<tr><td rowspan="2">TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability</td><td rowspan="2">✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-78</td><td>T1190: Exploit Public-Facing; T1059: Command and Scripting Interpreter</td><td>https://www.tp-link.com/us/support/faq/4308/</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-24363	✗	TP-Link TL-WA855RE V5 20200415-rel37464 devices	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:tp-link:tl-wa855re_firmware:*:*:*:*:*:*:*:*:* cpe:2.3:h:tp-link:tl-wa855re:v5:*:*:*:*:*:*:*:*	-
TP-link TL-WA855RE Missing Authentication for Critical Function Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://www.tp-link.com/us/support/download/tl-wa855re/v5.80/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-55177	✗	WhatsApp for iOS prior to v2.25.21.73, WhatsApp Business for iOS v2.25.21.78, WhatsApp for Mac v2.25.21.78	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:whatsapp:whatsapp:*:*:*:*:*:*:iphone_os:*:* cpe:2.3:a:whatsapp:whatsapp:*:*:*:*:*:*:macos:*:* cpe:2.3:a:whatsapp:whatsapp_business:*:*:*:*:*:*:iphone_os:*:*	-
Meta Platforms WhatsApp Incorrect Authorization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1204: User Execution; T1204.001: Malicious Link	https://www.whatsapp.com/download

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.

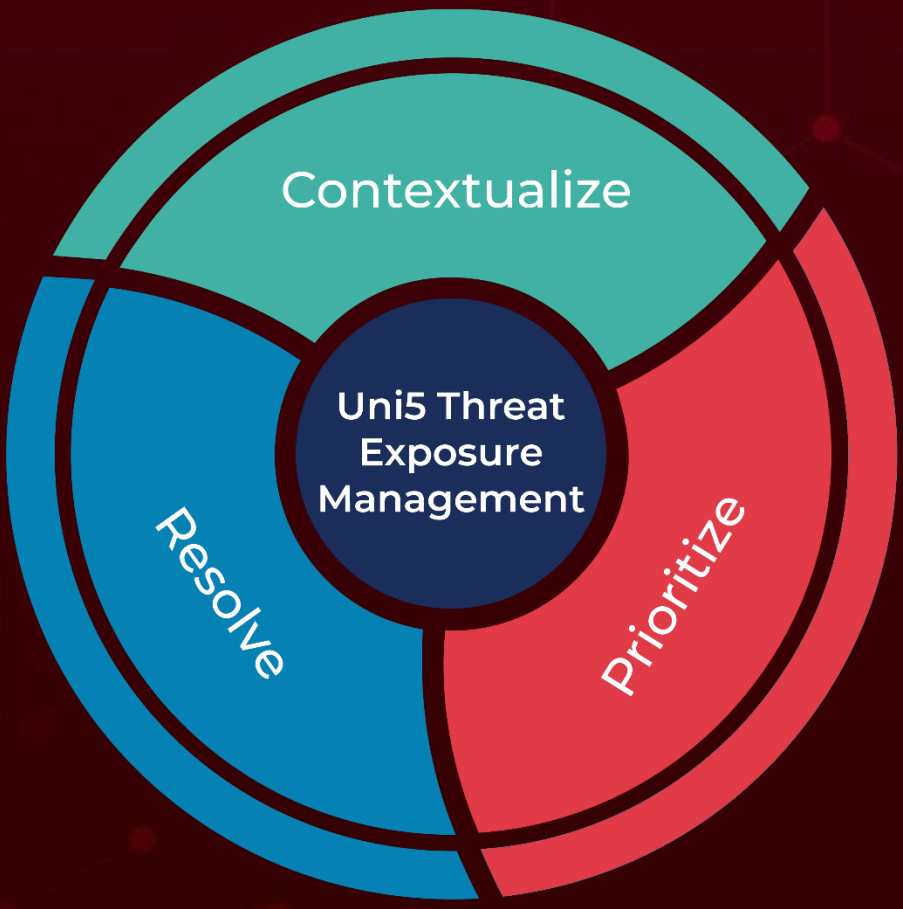
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

October 1, 2025 . 11:30 AM

More at www.hivepro.com