Date of Publication
September 2, 2025

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

August 2025

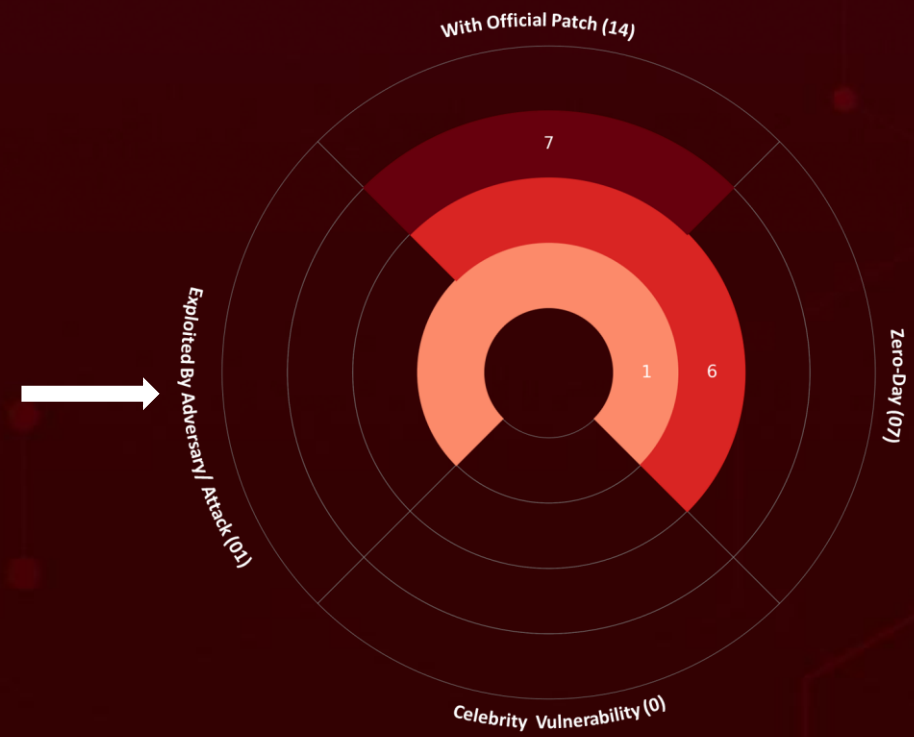
Table of Contents

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

15
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-57819	Sangoma FreePBX Authentication Bypass Vulnerability	Sangoma FreePBX	-	✓	✓	September 19, 2025
CVE-2025-7775	Citrix NetScaler Memory Overflow Vulnerability	Citrix NetScaler	9.8	✓	✓	August 28, 2025
CVE-2025-48384	Git Link Following Vulnerability	Git	8	✗	✓	September 15, 2025
CVE-2024-8068	Citrix Session Recording Improper Privilege Management Vulnerability	Citrix Session Recording	8	✗	✓	September 15, 2025
CVE-2024-8069	Citrix Session Recording Deserialization of Untrusted Data Vulnerability	Citrix Session Recording	8	✗	✓	September 15, 2025
CVE-2025-43300	Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability	Apple iOS, iPadOS, and macOS	8.8	✓	✓	September 11, 2025
CVE-2025-54948	Trend Micro Apex One OS Command Injection Vulnerability	Trend Micro Apex One	9.8	✓	✓	September 8, 2025
CVE-2025-8876	N-able N-Central Command Injection Vulnerability	N-able N-Central	8.8	✗	✓	August 20, 2025
CVE-2025-8875	N-able N-Central Insecure Deserialization Vulnerability	N-able N-Central	7.8	✗	✓	August 20, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2025-8088	RARLAB WinRAR Path Traversal Vulnerability	RARLAB WinRAR	8.8	✓	✓	September 2, 2025
CVE-2007-0671	Microsoft Office Excel Remote Code Execution Vulnerability	Microsoft Office	8.8	✓	✓	September 2, 2025
CVE-2013-3893	Microsoft Internet Explorer Resource Management Errors Vulnerability	Microsoft Internet Explorer	8.8	✓	✓	September 2, 2025
CVE-2020-25078	D-Link DCS-2530L and DCS-2670L Devices Unspecified Vulnerability	D-Link DCS-2530L and DCS-2670L Devices	7.5	✗	✓	August 26, 2025
CVE-2020-25079	D-Link DCS-2530L and DCS-2670L Command Injection Vulnerability	D-Link DCS-2530L and DCS-2670L Devices	8.8	✗	✓	August 26, 2025
CVE-2022-40799	D-Link DNR-322L Download of Code Without Integrity Check Vulnerability	D-Link DNR-322L	8.8	✗	EOL	August 26, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-57819	ZERO-DAY	FreePBX 15, 16, and 17	-
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sangoma:freepbx:*:*:*:*:*:*:*:*	-
Sangoma FreePBX Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89, CWE-288	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-7775</td><td>  </td><td rowspan="2">NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.48 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-59.22 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.241-FIPS and NDcPP NetScaler ADC 12.1-FIPS and NDcPP BEFORE 12.1-55.330-FIPS and NDcPP</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:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:*
cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*
cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:*
cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Citrix NetScaler Memory Overflow Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-119</td><td>T1059: Command and Scripting Interpreter, T1499: Endpoint Denial of Service, T1190: Exploit Public-Facing Application</td><td>https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_7775_CVE_2025_7776_and_CVE_2025_8424</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-2025-48384</td><td>✗</td><td rowspan="2">Git v2.50.0, v2.49.0, v2.48.0-v2.48.1, v2.47.0–v2.47.2, v2.46.0–v2.46.3, v2.45.0-v2.45.3, v2.44.0–v2.44.3, v2.43.6 and prior</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:git-scm:git:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Git Link Following Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-59, CWE-436</td><td>T1195: Supply Chain Compromise, T1059: Command and Scripting Interpreter</td><td>https://github.com/git/git/security/advisories/GHSA-vwqx-4fm8-6qc9</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-2024-8068</td><td>✗</td><td rowspan="2">Citrix Session RecordingCurrent Release (CR): Before: 2407 Hotfix 24.5.200.8 Long Term Service Release (LTSR):1912 LTSR: Affected versions before CU9 Hotfix 19.12.9100.6, 2203 LTSR: Affected versions before CU5 Hotfix 22.03.5100.11, 2402 LTSR: Affected versions before CU1 Hotfix 24.02.1200.16</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:citrix:session_recording:*:*:*:*:-:*:*:*
cpe:2.3:a:citrix:session_recording:2407:-:*:*:-:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Citrix Session Recording Improper Privilege Management Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-269</td><td>T1068: Exploitation for Privilege Escalation, T1548: Abuse Elevation Control Mechanism, T1078: Valid Accounts</td><td>https://support.citrix.com/external/article?articleUrl=CTX691941-citrix-session-recording-security-bulletin-for-cve20248068-and-cve20248069</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-2024-8069</td><td>  </td><td rowspan="2">Citrix Session Recording Current Release (CR): Before: 2407 Hotfix 24.5.200.8 Long Term Service Release (LTSR):1912 LTSR: Affected versions before CU9 Hotfix 19.12.9100.6, 2203 LTSR: Affected versions before CU5 Hotfix 22.03.5100.11, 2402 LTSR: Affected versions before CU1 Hotfix 24.02.1200.16</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:citrix:session_recording:*:*:*:*:-:*:*:*
cpe:2.3:a:citrix:session_recording:2407:-:*:*:-:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Citrix Session Recording Deserialization of Untrusted Data 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>T1068: Exploitation for Privilege Escalation, T1203: Exploitation for Client Execution</td><td>https://support.citrix.com/external/article?articleUrl=CTX691941-citrix-session-recording-security-bulletin-for-cve20248068-and-cve20248069</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-43300	✗	macOS: All versions before macOS Sequoia 15.6.1, macOS Sonoma 14.7.8, and macOS Ventura 13.7.8. iOS and iPadOS: All versions before iOS/iPadOS 18.6.2 and 17.7.10.	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	https://support.apple.com/en-us/124925, https://support.apple.com/en-us/124926, https://support.apple.com/en-us/124927, https://support.apple.com/en-us/124928, https://support.apple.com/en-us/124929

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-54948	✗	Trend Micro Apex One Management Server Version 14039 and below	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:trendmicro:apexone:*:*:*:*:*:*:*:*	-
Trend Micro Apex One OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting, T1203 : Exploitation for Client Execution	https://success.trendmicro.com/en-US/solution/KA-0020652

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-8876	✗	N-central: before 2025.3.1.	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	-
N-able N-Central Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78, CWE-20	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://status.n-able.com/2025/08/13/announcing-the-ga-of-n-central-2025-3-1/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-8875		N-central: before 2025.3.1.	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*:*:*	-
N-able N-Central Insecure Deserialization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	https://status.n-able.com/2025/08/13/announcing-the-ga-of-n-central-2025-3-1/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTORS
CVE-2025-8088		WinRAR Versions up to and including 7.12	RomCom, Paper Werewolf
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*	Mythic agents, SnipBot variants, and RustyClaw downloaders
RARLAB WinRAR Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-35	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-2007-0671		Microsoft Excel 2000, XP, 2003, and 2004 for Mac, and other Office products	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:excel:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:-:*:*:*:*:*:*:*	-
Microsoft Office Excel Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1204: User Execution, T1059: Command and Scripting Interpreter	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2007/ms07-015

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2013-3893		Microsoft Internet Explorer 6 through 11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:internet_explorer:-:*:*:*:*:*:*:*	-
Microsoft Internet Explorer Resource Management Errors Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-399, CWE-416	T1190: Exploit Public-Facing Application, T1204: User Execution, T1203: Exploitation for Client Execution	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-080

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-25078		D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dlink:dcs-4603_firmware:*:*:*:*:*:*:*:*cpe:2.3:h:dlink:dcs-4603:-:*:*:*:*:*:*:*	-
D-Link DCS-2530L and DCS-2670L Devices Unspecified Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10180

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-25079		D-Link DCS-2530L before 1.06.01 Hotfix and DCS-2670L through 2.02 devices	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dlink:dcs-4703e_firmware:*:*:*:*:*:*:*:*cpe:2.3:h:dlink:dcs-4703e:-:*:*:*:*:*:*:*	-
D-Link DCS-2530L and DCS-2670L Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1078: Valid Accounts	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10180

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-40799		D-Link DNR-322L devices running firmware version 2.60 Build 15 or earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dlink:dnr-322l_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:dlink:dnr-322l:-:*:*:*:*:*:*:*	-
D-Link DNR-322L Download of Code Without Integrity Check Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-494	T1059: Command and Scripting Interpreter, T1078: Valid Accounts	EOL

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.

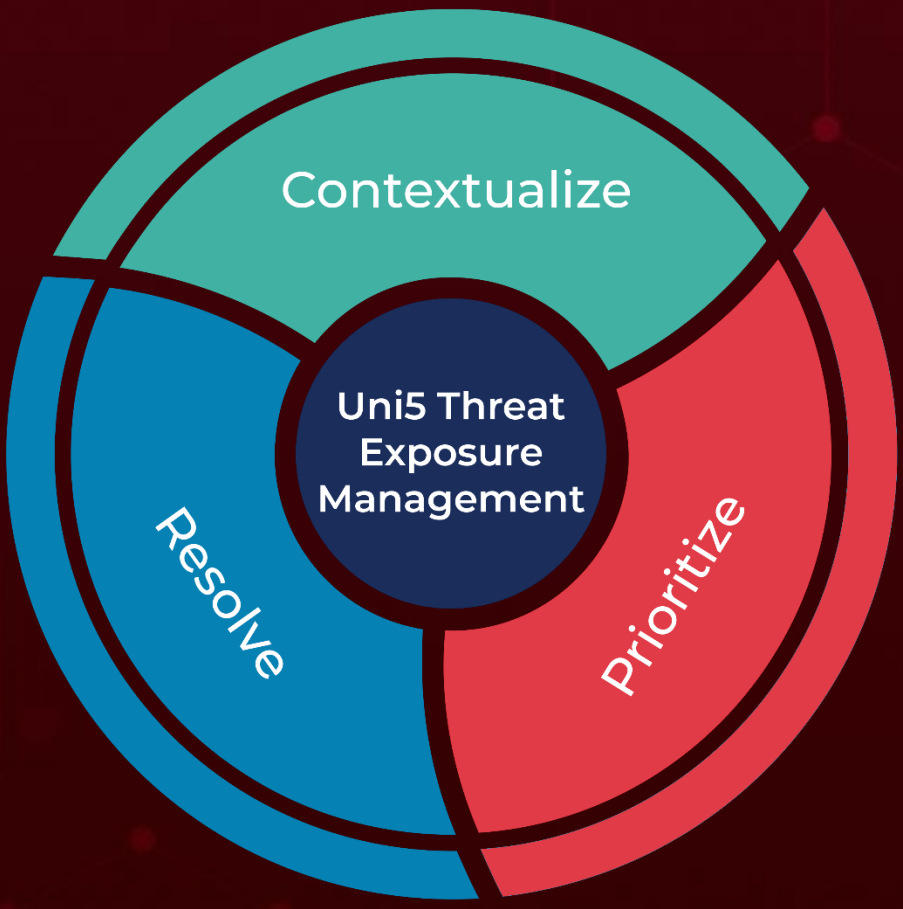
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

September 2, 2025 . 9:30 PM

More at www.hivepro.com