Date of Publication
May 5, 2025

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

April 2025

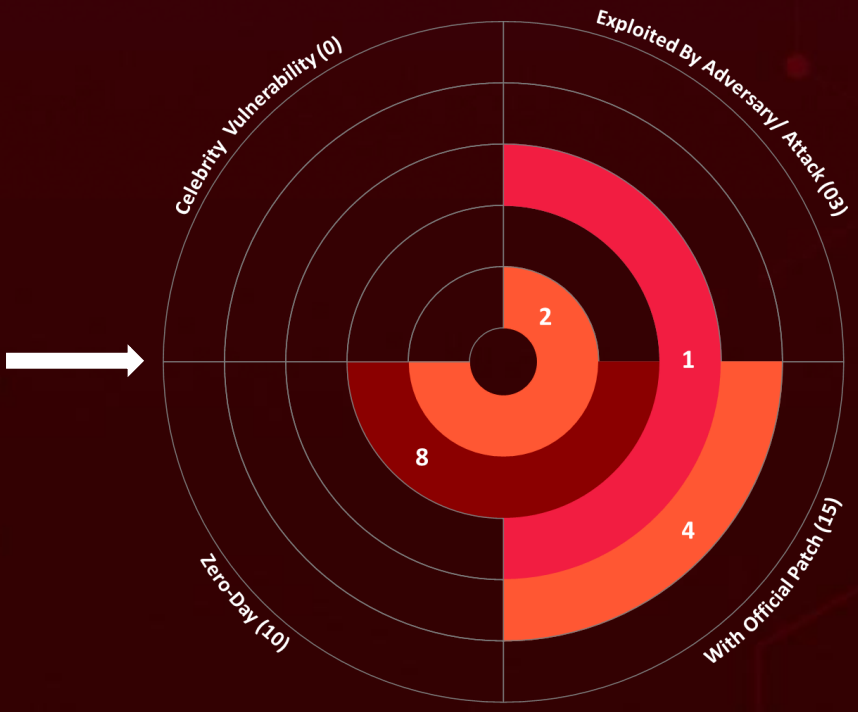
Table of Contents

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 April 2025, **fifteen** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **ten** are **zero-day** vulnerabilities; **three** have 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-2025-31324	SAP NetWeaver Unrestricted File Upload Vulnerability	SAP NetWeaver	10	✓	✓	May 20, 2025
CVE-2025-1976	Broadcom Brocade Fabric OS Code Injection Vulnerability	Broadcom Brocade Fabric OS	6.7	✓	✓	May 19, 2025
CVE-2025-42599	Qualitia Active! Mail Stack-Based Buffer Overflow Vulnerability	Qualitia Active! Mail	9.8	✓	✓	May 19, 2025
CVE-2025-3928	Commvault Web Server Unspecified Vulnerability	Commvault Web Server	8.8	✓	✓	May 19, 2025
CVE-2025-24054	Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability	Microsoft Windows	5.4	✗	✓	May 8, 2025
CVE-2025-31201	Apple Multiple Products Arbitrary Read and Write Vulnerability	Apple Multiple Products	6.8	✓	✓	May 8, 2025
CVE-2025-31200	Apple Multiple Products Memory Corruption Vulnerability	Apple Multiple Products	7.5	✓	✓	May 8, 2025
CVE-2021-20035	SonicWall SMA100 Appliances OS Command Injection Vulnerability	SonicWall SMA100 Appliances	6.5	✗	✓	May 7, 2025
CVE-2024-53150	Linux Kernel Out-of-Bounds Read Vulnerability	Linux Kernel	7.1	✓	✓	April 30, 2025
CVE-2024-53197	Linux Kernel Out-of-Bounds Access Vulnerability	Linux Kernel	7.8	✓	✓	April 30, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2025-29824	Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability	Microsoft Windows	7.8	✓	✓	April 29, 2025
CVE-2025-30406	Gladinet CentreStack and Triofox Use of Hard-coded Cryptographic Key Vulnerability	Gladinet CentreStack	9.8	✓	✓	April 29, 2025
CVE-2025-31161	CrushFTP Authentication Bypass Vulnerability	CrushFTP	9.8	✗	✓	April 28, 2025
CVE-2025-22457	Ivanti Connect Secure, Policy Secure and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure and ZTA Gateways	9.8	✗	✓	April 11, 2025
CVE-2025-24813	Apache Tomcat Path Equivalence Vulnerability	Apache Tomcat	9.8	✗	✓	April 22, 2025

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-31324	✗	SAP NetWeaver Version 7.50	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sap:sap_netweaver:7.50:*:*:*:*:*:*:*	-
SAP NetWeaver Unrestricted File Upload Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1505: Server Software Component; T1505.003: Web Shell; T1068: Exploitation for Privilege Escalation; T1562: Impair Defenses	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2025.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-1976	✗	Brocade Fabric OS versions 9.1.0 through 9.1.1d6.	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:broadcom:fabric_operating_system:*:*:*:*:*:*:*:*	-
Broadcom Brocade Fabric OS Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78, CWE-94	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25602

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-42599	✗	Active! mail 6 BuildInfo: 6.60.05008561 and earlier	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:qualitia:active_mail:*:*:*:*:*:*:*:*	-
Qualitia Active! Mail Stack-Based Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-121	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1499: Endpoint Denial of Service	https://jvn.jp/en/jp/JVN22348866/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-3928	✗	Commvault Version 11.36.0 - 11.36.45, 11.32.0 - 11.32.88, 11.28.0 - 11.28.140, 11.20.0 - 11.20.216	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:commvault:commvault:*:*:*:*:*:*:*:*	-
Commvault Web Server Unspecified Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1505: Server Software Component; T1505.003: Web Shell; T1059: Command and Scripting Interpreter; T1078: Valid Accounts	https://documentation.commvault.com/11.20/download_software.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-2025-24054</td><td>✗</td><td rowspan="2">Windows: 10 - 11 24H2, Windows Server: 2008 - 2025</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:microsoft:windows:*:*:*:*:*:*:*:*
cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-73</td><td>T1586: Compromise Accounts; T1040: Network Sniffing; T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24054</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-2025-31201</td><td>  </td><td rowspan="2">macOS Prior to Version 15.4.1 iOS and iPadOS Prior to Version 18.4.1 tvOS Prior to Version 18.4.1 visionOS Prior to Version 2.4.1</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:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Apple Multiple Products Arbitrary Read and Write Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td></td><td>CWE-287</td><td>T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution; T1068: Exploitation for Privilege Escalation</td><td>https://support.apple.com/en-us/108382, https://support.apple.com/en-us/118575, https://support.apple.com/en-us/108414, https://support.apple.com/en-us/118481</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-31200		macOS Prior to Version 15.4.1 iOS and iPadOS Prior to Version 18.4.1 tvOS Prior to Version 18.4.1 visionOS Prior to Version 2.4.1	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	-
Apple Multiple Products Memory Corruption Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINKS**
	CWE-787	T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution; T1068: Exploitation for Privilege Escalation	https://support.apple.com/en-us/108382, https://support.apple.com/en-us/118575, https://support.apple.com/en-us/108414, https://support.apple.com/en-us/118481

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-20035	✗	SMA100 management interface 9.0.0.10-28sv and earlier, 10.2.0.7-34sv and earlier, 10.2.1.0-17sv and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:sonicwall:sma_200_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:sonicwall:sma_200:-:*:*:*:*:*:*:*	-
SonicWall SMA100 Appliances OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1498: Network Denial of Service; T1059: Command and Scripting Interpreter	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0022

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53150	✗	Linux kernel from version 5.4 up to versions before 6.12.2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:*	-
Linux Kernel Out-of-Bounds Read Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1068: Exploitation for Privilege Escalation; T1574: Hijack Execution Flow	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=096bb5b43edf755bc4477e64004fa3a20539ec2f

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53197		Linux Kernel	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	NoviSpy
Linux Kernel Out-of-Bounds Access Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation; T1574: Hijack Execution Flow	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=0b4ea4bfe16566b84645ded1403756a2dc4e0f19

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-29824		Windows: 10 - 11 24H2, Windows Server: 2008 - 2025	Storm-2460
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	PipeMagic
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/vulnerability/CVE-2025-29824

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30406	✗	Gladinet CentreStack through 16.1.10296.56315	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gladinet:centrestack:*:*:*:*:*:*:*:*	-
Gladinet CentreStack and Triofox Use of Hard-coded Cryptographic Key Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-321, CWE-798	T1552: Unsecured Credentials; T1552.004: Private Keys; T1190 : Exploit Public-Facing Application	https://www.centrestack.com/p/gce_latest_release.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-31161	✗	CrushFTP versions 10.0.0 through 10.8.3 and 11.0.0 through 11.3.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*:*:*	-
CrushFTP Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-305	T1556: Modify Authentication Process	https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update, https://www.crushftp.com/download.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-22457	✗	Ivanti Connect Secure: 22.7R2.5 and prior Pulse Connect Secure (EoS): 9.1R18.9 and prior Ivanti Policy Secure: 22.7R1.3 and prior ZTA Gateways: 22.8R2 and prior	UNC5221
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*:*	TRAILBLAZE, BRUSHFIRE, SPAWNSNARE, SPAWNWAVE, SPAWNSLOTH
Ivanti Connect Secure, Policy Secure and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-121	T1190: Exploit Public-Facing Application; T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-24813</td><td>✗</td><td rowspan="2">Apache Tomcat Versions 11.0.0-M1 to 11.0.2, Apache Tomcat Versions 10.1.0-M1 to 10.1.34, Apache Tomcat Versions 9.0.0.M1 to 9.0.98</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:apache:tomcat:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Apache Tomcat Path Equivalence Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-44, CWE-502</td><td>T1059: Command and Scripting Interpreter; T1203: Exploitation for Client Execution</td><td>https://tomcat.apache.org/security-11.html, https://tomcat.apache.org/security-10.html, https://tomcat.apache.org/security-9.html</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.

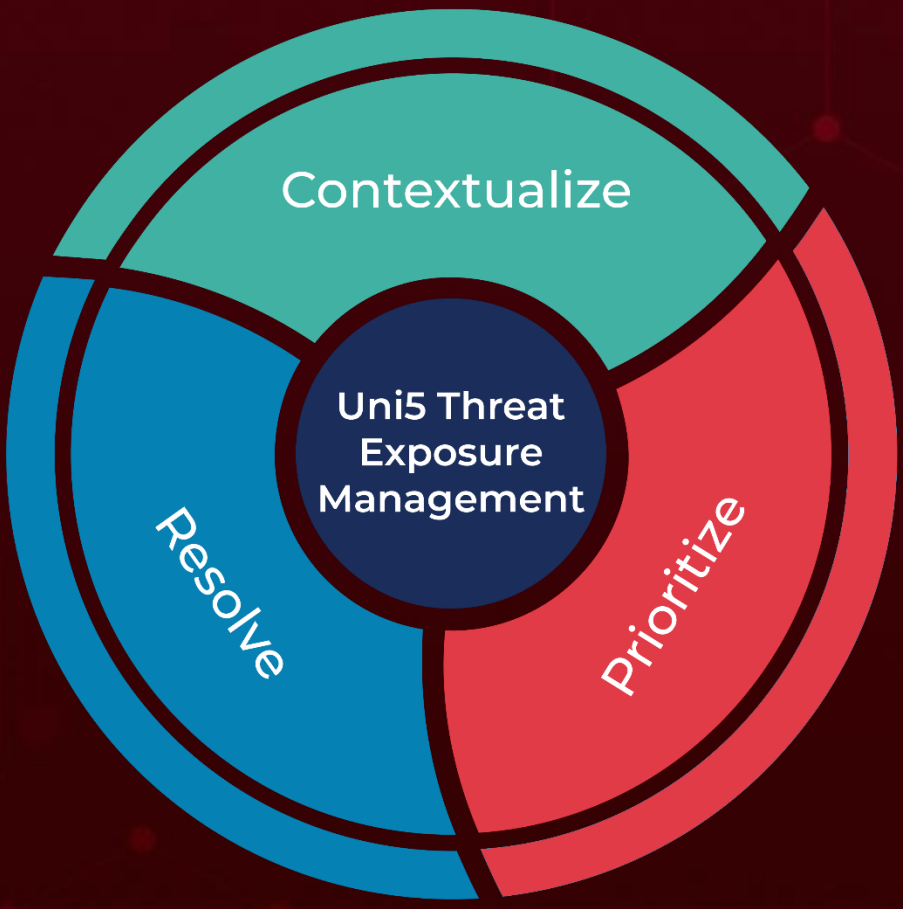
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

May 5, 2025 . 4:30 AM

More at www.hivepro.com