Date of Publication
September 3, 2024

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

August 2024

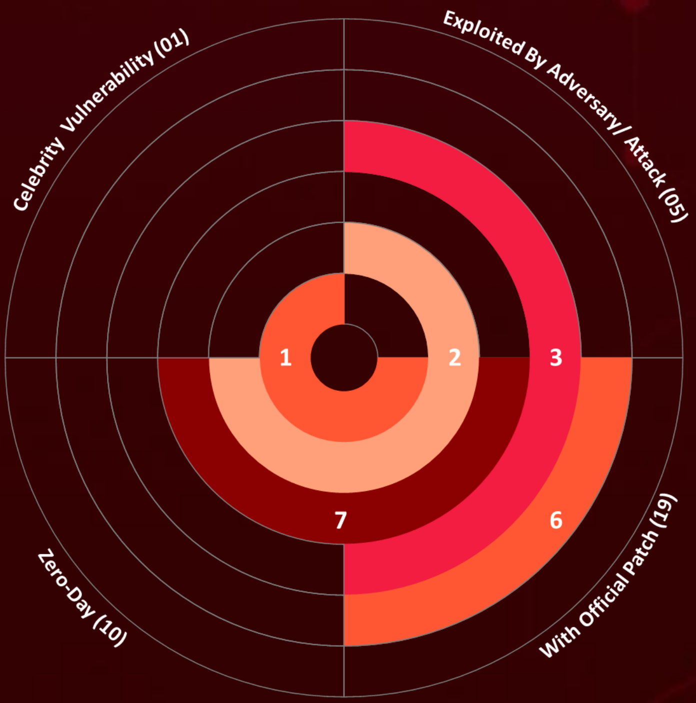
Table of Contents

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 2024, **nineteen** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **ten** are **zero-day** vulnerabilities; **five** have been **exploited** by known threat actors and employed in attacks.

19
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2018-0824	Microsoft COM for Windows Deserialization of Untrusted Data Vulnerability	Microsoft Windows	8.8	✗	✓	August 26, 2024
CVE-2024-32113	Apache OFBiz Path Traversal Vulnerability	Apache OFBiz	9.8	✗	✓	August 28, 2024
CVE-2024-36971	Android Kernel Remote Code Execution Vulnerability	Android Kernel	7.8	✓	✓	August 28, 2024
CVE-2024-38107	Microsoft Windows Power Dependency Coordinator Privilege Escalation Vulnerability	Microsoft Windows	7.8	✓	✓	September 3, 2024
CVE-2024-38106	Microsoft Windows Kernel Privilege Escalation Vulnerability	Microsoft Windows	7	✓	✓	September 3, 2024
CVE-2024-38193	Microsoft Windows Ancillary Function Driver for WinSock Privilege Escalation Vulnerability	Microsoft Windows	7.8	✓	✓	September 3, 2024
CVE-2024-38213	Copy2Pwn (Microsoft Windows SmartScreen Security Feature Bypass Vulnerability)	Microsoft Windows	6.5	✓	✓	September 3, 2024
CVE-2024-38178	Microsoft Windows Scripting Engine Memory Corruption Vulnerability	Microsoft Windows	7.5	✓	✓	September 3, 2024
CVE-2024-38189	Microsoft Project Remote Code Execution Vulnerability	Microsoft Project	8.8	✓	✓	September 3, 2024

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-28986	SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability	SolarWinds Web Help Desk	9.8	✗	✓	September 5, 2024
CVE-2024-23897	Jenkins Command Line Interface (CLI) Path Traversal Vulnerability	Jenkins Command Line Interface (CLI)	9.8	✗	✓	September 9, 2024
CVE-2021-31196	Microsoft Exchange Server Information Disclosure Vulnerability	Microsoft Exchange Server	7.2	✗	✓	September 11, 2024
CVE-2022-0185	Linux Kernel Heap-Based Buffer Overflow	Linux Kernel	8.4	✗	✓	September 11, 2024
CVE-2021-33045	Dahua IP Camera Authentication Bypass Vulnerability	Dahua IP Camera Firmware	9.8	✗	✓	September 11, 2024
CVE-2021-33044	Dahua IP Camera Authentication Bypass Vulnerability	Dahua IP Camera Firmware	9.8	✗	✓	September 11, 2024
CVE-2024-39717	Versa Director Dangerous File Type Upload Vulnerability	Versa Director	7.2	✓	✓	September 13, 2024
CVE-2024-7971	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8	8.8	✓	✓	September 16, 2024
CVE-2024-38856	Apache OFBiz Incorrect Authorization Vulnerability	Apache OFBiz	9.8	✗	✓	September 17, 2024
CVE-2024-7965	Google Chromium V8 Inappropriate Implementation Vulnerability	Google Chromium V8	8.8	✓	✓	September 18, 2024

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-0824	⊗	Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.	APT41
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	ShadowPad
Microsoft COM for Windows Deserialization of Untrusted Data Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1204: User Execution, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0824

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-32113</td><td>✗</td><td rowspan="2">Apache OFBiz version before 18.12.13</td><td rowspan="2">-</td></tr>
<tr><td><b>ZERO-DAY</b></td></tr>
<tr><td>✗</td><td><b>AFFECTED CPE</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td></tr>
<tr><td><b>NAME</b></td><td><b>BAS ATTACKS</b></td><td rowspan="2">cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Apache OFBiz Path Traversal Vulnerability</td><td>✗</td></tr>
<tr><td><b>CWE ID</b></td><td><b>ASSOCIATED TTPs</b></td><td><b>PATCH LINKS</b></td></tr>
<tr><td>CWE-22</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://issues.apache.org/jira/browse/OFBIZ-13006
https://ofbiz.apache.org/security.html</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-2024-36971</td><td>✗</td><td rowspan="2">Linux Kernal</td><td rowspan="2">-</td></tr>
<tr><td><b>ZERO-DAY</b></td></tr>
<tr><td>✓</td><td><b>AFFECTED CPE</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td></tr>
<tr><td><b>NAME</b></td><td><b>BAS ATTACKS</b></td><td rowspan="2">cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Android Kernel Remote Code Execution Vulnerability</td><td>✗</td></tr>
<tr><td><b>CWE ID</b></td><td><b>ASSOCIATED TTPs</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>CWE-416</td><td>T1059: Command and Scripting Interpreter</td><td>https://source.android.com/docs/security/bulletin/2024-08-01</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38107	✗	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23 H2	-
	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 Power Dependency Coordinator Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38106	✗	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23 H2	-
	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 Kernel Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-591	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38193	✗	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	-
	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 Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38213	✓	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Copy2Pwn (Microsoft Windows SmartScreen Security Feature Bypass Vulnerability)	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1204: User Execution, T1204.002: Malicious File, T1562: Impair Defenses	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38178	✗	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	-
	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 Scripting Engine Memory Corruption Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1204: User Execution, T1204.001: Malicious Link, T1562: Impair Defenses, T1562.010: Downgrade Attack	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38189	✗	Microsoft Office LTSC 2021, Microsoft Project, Microsoft 365 Apps for Enterprise	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:365_apps:-:*:*:*:enterprise:*:*:* cpe:2.3:a:microsoft:office:-:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:project:*:*:*:*:*:*:*:*	-
Microsoft Project Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1204: User Execution, T1204.002: Malicious File	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28986	✗	SolarWinds Web Help Desk 12.8.3 and all previous versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:solarwinds:web_help_desk:*:*:*:*:*:*:*:*	-
SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://support.solarwinds.com/SuccessCenter/s/article/WHD-12-8-3-Hotfix-1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23897	✗	Jenkins: 2.204.2 - 2.441 Jenkins LTS: 2.222.1 - 2.426.2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:jenkins:jenkinsLTS:*:*:*:*:*:*:*	-
Jenkins Command Line Interface (CLI) Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22 CWE-27	T1059: Command and Scripting Interpreter	https://www.jenkins.io/security/advisory/2024-01-24/#SECURITY-3314

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-31196	✗	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002	Unknown Iranian attackers
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:exchange_server:cumulative_update:*:*:*:*:*:*	-
Microsoft Exchange Server Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31196

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-0185	✗	FAS/AFF BMC, NetApp HCI BMC	UNC5174 (aka Uteus)
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	SNOWLIGHT, GOHEAVY, GOREVERSE, SUPERSHELL
Linux Kernel Heap-Based Buffer Overflow	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-191 CWE-190	T1574: Hijack Execution Flow, T1211: Exploitation for Defense Evasion	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-33045	✗	Dahuasecurity Ipc-hum7xxx_firmware before 2.820.0000000.5.r.210705	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dahuasecurity:ipc-hum7xxx_firmware:*:*:*:*:*:*:*:*	-
Dahua IP Camera Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1556: Modify Authentication Process	https://www.dahuasecurity.com/support/cybersecurity/details/957

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-33044	✗	Dahuasecurity Ipc-hum7xxx_firmware before 2.820.0000000.5.r.210705	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dahuasecurity:ipc-hum7xxx_firmware:*:*:*:*:*:*:*:*	-
Dahua IP Camera Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1556: Modify Authentication Process	https://www.dahuasecurity.com/support/cybersecurity/details/957

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-39717	✗	Versa Director: 21.2.3 - 22.1.3	Volt Typhoon
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:versa-networks:versa_director:-:*:*:*:*:*:*:*	VersaMem
	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
Versa Director Dangerous File Type Upload Vulnerability	CWE-434	T1190: Exploit Public-Facing Application, T1036.008: Masquerade File Type, T1055: Process Injection	https://versa-networks.com/blog/versa-security-bulletin-update-on-cve-2024-39717-versa-director-dangerous-file-type-upload-vulnerability/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7971	✗	Google Chrome: 100.0.4896.60 - 127.0.6533.120	Citrine Sleet
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:*	FudModule Rootkit
	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
Google Chromium V8 Type Confusion Vulnerability	CWE-843	T1189: Drive-by Compromise, T1204: User execution	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38856	✗	OFBiz: 4.0 - 22.01.01	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*:*:*	-
Apache OFBiz Incorrect Authorization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1068: Exploitation for Privilege Escalation, T1556: Modify Authentication Process, T1059: Command and Scripting Interpreter	https://ofbiz.apache.org/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7965	✗	Google Chrome: 100.0.4896.60 - 127.0.6533.120	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium V8 Inappropriate Implementation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787 CWE-358	T1204.001: Malicious Link, T1189: Drive-by Compromise	https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html

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.

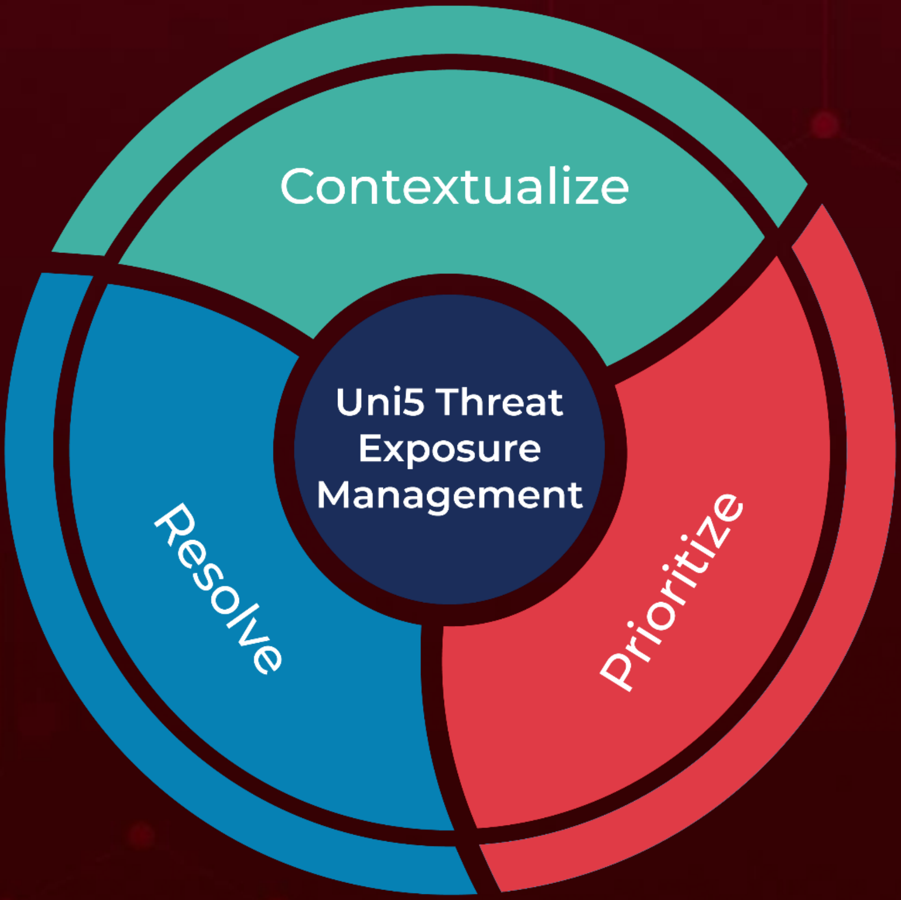
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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 3, 2024 • 10:30 PM

More at www.hivepro.com