Date of Publication
December 1, 2023

Hive Pro®

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

November 2023

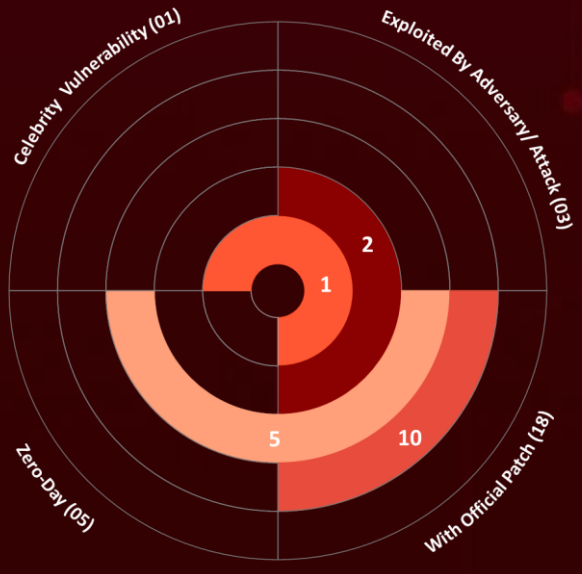
Table of Contents

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 November 2023, eighteen vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, five are zero-day vulnerabilities; three have been exploited by known threat actors and employed in attacks.

18
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-46604	Apache ActiveMQ Deserialization of Untrusted Data Vulnerability	Apache ActiveMQ	9.8	✗	✓	November 23, 2023
CVE-2023-22518	Atlassian Confluence Data Center and Server Improper Authorization Vulnerability	Atlassian Confluence Data Center and Server	9.8	✗	✓	November 24, 2023
CVE-2023-29552	Service Location Protocol (SLP) Denial-of-Service Vulnerability	IETF Service Location Protocol (SLP)	7.5	✗	✗	November 25, 2023
CVE-2023-47246	SysAid Server Path Traversal Vulnerability	SysAid SysAid Server	9.8	✓	✓	November 26, 2023
CVE-2023-36844	Juniper Junos OS EX Series PHP External Variable Modification Vulnerability	Juniper Junos OS	5.3	✗	✓	November 27, 2023
CVE-2023-36845	Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability	Juniper Junos OS	9.8	✗	✓	November 28, 2023
CVE-2023-36846	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability	Juniper Junos OS	5.3	✗	✓	November 29, 2023
CVE-2023-36847	Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability	Juniper Junos OS	5.3	✗	✓	November 30, 2023
CVE-2023-36851	Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability	Juniper Junos OS	5.3	✗	✓	December 1, 2023

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-36033	Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability	Microsoft Windows	7.8	✓	✓	December 2, 2023
CVE-2023-36025	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	8.8	✓	✓	December 3, 2023
CVE-2023-36036	Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability	Microsoft Windows	7.8	✓	✓	December 4, 2023
CVE-2023-36584	Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability	Microsoft Windows	5.4	✗	✓	December 5, 2023
CVE-2023-1671	Sophos Web Appliance Command Injection Vulnerability	Sophos Web Appliance	9.8	✗	✓	December 6, 2023
CVE-2020-2551	Oracle Fusion Middleware Unspecified Vulnerability	Oracle Fusion Middleware	9.8	✗	✓	December 7, 2023
CVE-2023-4911	GNU C Library Buffer Overflow Vulnerability	GNU GNU C Library	7.8	✗	✓	December 8, 2023
CVE-2023-6345	Google Skia Integer Overflow Vulnerability	Google Skia	-	✓	✓	December 9, 2023
CVE-2023-49103	ownCloud graphapi Information Disclosure Vulnerability	ownCloud ownCloud graphapi	10	✗	✓	December 10, 2023

CVEs Details

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="4">CVE-2023-46604</td><td>  </td><td rowspan="3">Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16</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:apache:activemq:*:*:*:*:*:*:*
cpe:2.3:a:apache:activemq_legacy_openwire_module:*:*:*:*:*:*:*:*</td><td rowspan="2">Kinsing, HelloKitty ransomware, GoTitan Botnet</td></tr>
<tr><td rowspan="3">Apache ActiveMQ 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>T1059: Command and Scripting Interpreter</td><td>https://activemq.apache.org/security-advisories.data/CVE-2023-46604</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22518	✗	Confluence Data Center and Server 6.0.1 - 8.6.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:atlassian:confluence_server_and_data_center:8.6.0:*:*:*:*:*:*:*	Cerber Ransomware
Atlassian Confluence Improper Authorization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-285	T1059: Command and Scripting Interpreter, T1204: User Execution	https://www.atlassian.com/software/confluence/download-archives

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29552	✗	Service Location Protocol version: 2.0.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:service_location_protocol:service_location_protocol:*:*:*:*:*:*:*:*	-
Service Location Protocol (SLP) Denial-of-Service Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-345	T1498: Network Denial of Service	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-47246	✗	SysAid Server Path Traversal Vulnerability	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sysaid:sysaid:-:*:*:*:*:*:*:*	-
SysAid Server Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1083: File and Directory Discovery	https://documentation.sysaid.com/docs/latest-version-installation-files

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36844	✗	Juniper Junos OS: 20.4 - 22.4R2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*	-
Juniper Junos OS EX Series PHP External Variable Modification Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-473	T1005: Data from Local System, T1499.004: Application or System Exploitation, T1211: Exploitation for Defense Evasion	https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36845	✗	Juniper Junos OS: 20.4 - 22.4R2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*	-
Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-473	T1005: Data from Local System, T1499.004: Application or System Exploitation, T1211: Exploitation for Defense Evasion	https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-36846</td><td>✗</td><td rowspan="2">Juniper Junos OS: 20.4 - 22.4R2</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:juniper:junos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-306</td><td>T1190: Exploit Public-Facing Application, T1040: Network Sniffing</td><td>https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US</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-2023-36847</td><td>✗</td><td rowspan="2">Juniper Junos OS: 20.4 - 22.4R2</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:juniper:junos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-306</td><td>T1190: Exploit Public-Facing Application, T1040: Network Sniffing</td><td>https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US</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-2023-36851</td><td>✗</td><td rowspan="2">Juniper Junos OS: 20.4 - 22.4R2</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:juniper:junos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>WORKAROUND</td></tr>
<tr><td>CWE-306</td><td>T1190: Exploit Public-Facing Application, T1040: Network Sniffing</td><td>https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36033	✗	Windows: 10 - 11 23H2, Windows Server: 2019 - 2022 23H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	-
Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1068: Exploitation for Privilege Escalation, T1204.001: Malicious Link	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36033

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36025	✗	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:10:1809:*:*:*:*:*:*:*	-
Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36025

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36036	✗	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:10:1809:*:*:*:*:*:*:*	-
Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1068: Exploitation for Privilege Escalation, T1204.001: Malicious Link	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36036

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36584	✗	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_10_1507:*:*:*:*:*:*:x64:*	-
Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36584

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-1671		Sophos Web Appliance (SWA): before 4.3.10.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sophos:swa:*:*:*:*:*:*:*:*	-
Sophos Web Appliance Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://www.sophos.com/en-us/security-advisories/sophos-sa-20230404-swa-rce

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-2551		Oracle WebLogic Server: 10.3.6.0.0 - 12.2.1.4.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:oracle_weblogic_server:10.3.6.0.0:*:*:*:*:*:*:*	-
Oracle Fusion Middleware Unspecified Vulnerability			
	CWE ID	ASSOCIATED TTPs	WORKAROUND
	CWE-20	T1059: Command and Scripting Interpreter	https://www.oracle.com/security-alerts/cpujan2020.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4911	Looney Tunables	All systems running glibc 2.34 to 2.37	Kinsing (aka Money Libra)
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gnu:c_library:*:*:*:*:*:*:*:*	-
GNU C Library Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1068: Exploitation for Privilege Escalation	Upgrade glibc to 2.38 or later versions

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-6345	✗	Google Chrome: 100.0.4896.60 - 119.0.6045.160	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Skia Integer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1059: Command and Scripting Interpreter	https://www.google.com/intl/en/chrome/?standalone=1

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-49103</td><td>  </td><td rowspan="2">ownCloud graphapi 0.2.0 – 0.3.0</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:owncloud:graphapi:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">ownCloud graphapi Information Disclosure Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-200</td><td>T1589.001: Credentials, T1589: Gather Victim Identity Information</td><td>https://marketplace.owncloud.com/apps/graphapi</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 impact are profound and multifaceted. These vulnerabilities provide malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information. This is also known as Celebrity Publicized Software Flaws.

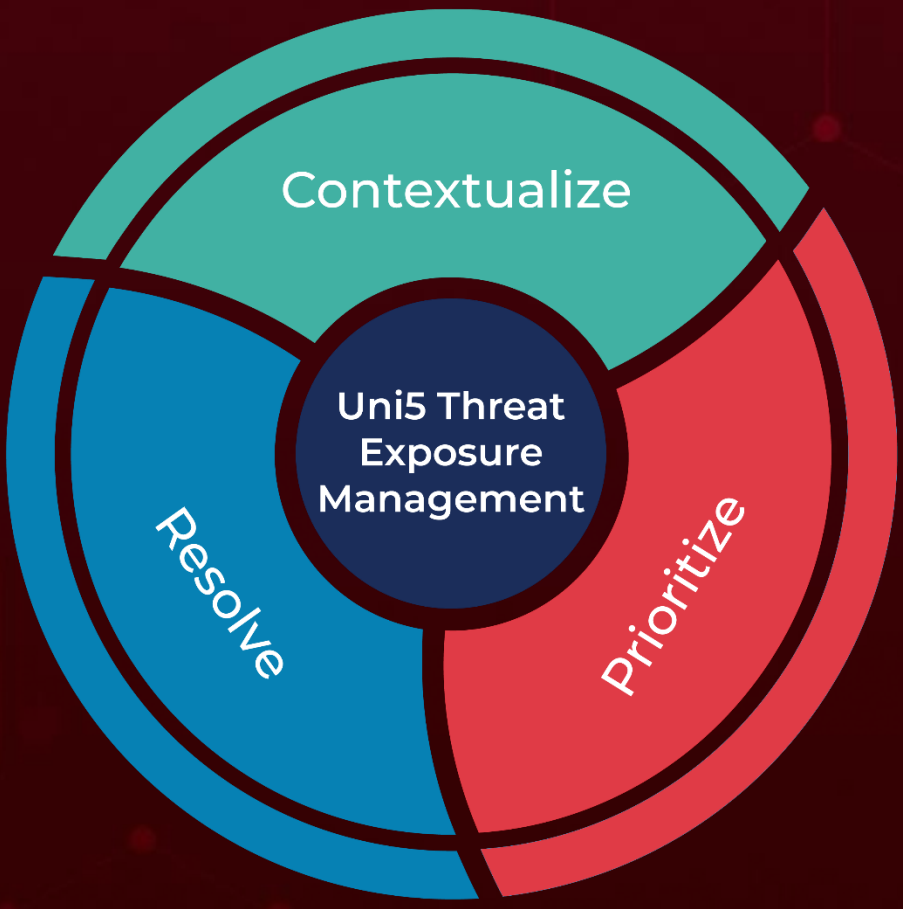
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

December 1, 2023 . 7:00 AM

More at www.hivepro.com