Date of Publication
April 01, 2023

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

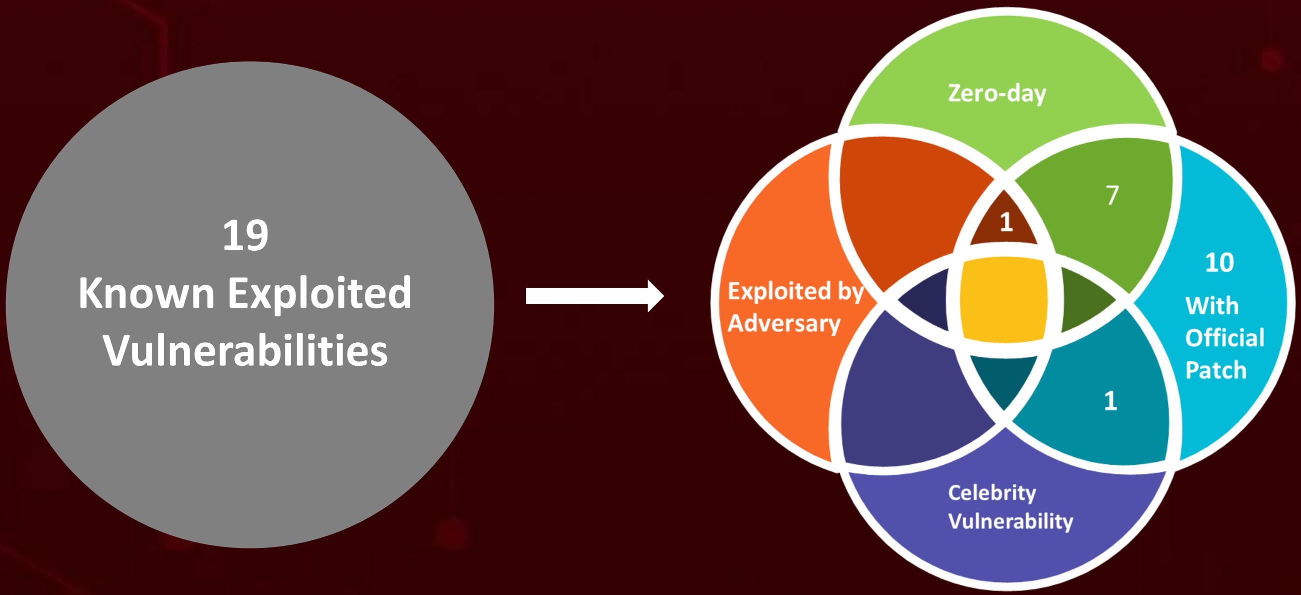
March 2023

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 March 2023, nineteen vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Out of the 19 vulnerabilities, eight are zero-day, and one has been exploited by an unknown Russian threat actor. Another zero-day exploit has been exploited by UNC3886.



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2022-35914	Teclib GLPI Remote Code Execution Vulnerability	Teclib GLPI	9.8	✗	✓	March 28, 2023
CVE-2022-33891	Apache Spark Command Injection Vulnerability	Apache Spark	8.8	✗	✓	March 28, 2023
CVE-2022-28810	Zoho ManageEngine ADSelfService Plus Remote Code Execution Vulnerability	Zoho ManageEngine	6.8	✗	✓	March 28, 2023
CVE-2020-5741	Plex Media Server Remote Code Execution Vulnerability	Plex Media Server	7.2	✗	✓	March 31, 2023
CVE-2021-39144	XStream Remote Code Execution Vulnerability	XStream	8.5	✗	✓	March 31, 2023
CVE-2022-41328	Fortinet FortiOS Path Traversal Vulnerability	Fortinet FortiOS	7.1	✓	✓	April 04, 2023
CVE-2023-24880	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	4.4	✓	✓	April 04, 2023
CVE-2023-23397	Microsoft Office Outlook Privilege Escalation Vulnerability	Microsoft Office	9.8	✓	✓	April 04, 2023
CVE-2023-26360	Adobe ColdFusion Improper Access Control Vulnerability	Adobe ColdFusion	9.8	✓	✓	April 05, 2023

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2013-3163	Microsoft Internet Explorer Memory Corruption Vulnerability	Microsoft Internet Explorer	-	✓	✓	April 20, 2023
CVE-2014-1776	Microsoft Internet Explorer Memory Corruption Vulnerability	Microsoft Internet Explorer	-	✓	✓	April 20, 2023
CVE-2017-7494	Samba Remote Code Execution Vulnerability	Samba	9.8	✗	✓	April 20, 2023
CVE-2022-42948	Fortra Cobalt Strike User Interface Remote Code Execution Vulnerability	Fortra Cobalt Strike	9.8	✗	✓	April 20, 2023
CVE-2022-39197	Fortra Cobalt Strike Teamserver Cross-Site Scripting (XSS) Vulnerability	Fortra Cobalt Strike	6.1	✗	✓	April 20, 2023
CVE-2021-30900	Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability	AppleiOS, iPadOS, and macOS	7.8	✗	✓	April 20, 2023
CVE-2022-38181	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	ArmMali Graphics Processing Unit (GPU)	8.8	✗	✓	April 20, 2023
CVE-2023-0266	Linux Kernel Use-After-Free Vulnerability	Linux Kernel	7.8	✓	✓	April 20, 2023
CVE-2022-3038	Google Chrome Use-After-Free Vulnerability	Google Chrome	8.8	✗	✓	April 20, 2023
CVE-2022-22706	Arm Mali GPU Kernel Driver Unspecified Vulnerability	Arm Mali Graphics Processing Unit (GPU)	7.8	✓	✓	April 20, 2023

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-35914	✗	GLPI: 10.0.0 - 10.0.2, 9.1 - 9.5.8	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:glpi-project:glpi:*:*:*:*:*:*:*:*	-
Teclib GLPI Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1203: Exploitation for Client Execution	http://www.bioinformatics.org/phplabware/sourceer/sourceer.php?&Sfs=htmLawedTest.php&Sl=.%2Finternal_utilities%2FhtmLawed

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-33891	✗	Apache Spark Versions 3.0.3 and earlier, 3.1.1 to 3.1.2, and 3.2.0 to 3.2.1.	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:spark:*:*:*:*:*:*:*:*	Zerobot
Apache Spark Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1623: Command and Scripting Interpreter T1203: Exploitation for Client Execution	https://lists.apache.org/thread/p847l3kopoo5bjtmxcwk21xp6tjxqlc

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-28810	✗	Zoho ManageEngine ADSelfService Plus: 6100 - 6121	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:zohocorp:zoho_manageengine_adselfservice_plus:6121:*:*:*:*:*:*:*	-
Zoho ManageEngine ADSelfService Plus Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1203: Exploitation for Client Execution	https://www.manageengine.com/products/self-service-password/kb/cve-2022-28810.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-5741	✗	Plex Media Server: before 1.19.3	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:*	-
Plex Media Server Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059.006: Command and Scripting Interpreter: Python	https://forums.plex.tv/t/security-regarding-cve-2020-5741/586819

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2021-39144]()	✗	Ubuntu: 22.10, 22.04, 20.04, 18.04, 16.04, 14.04 libxstream-java (Ubuntu package): before Ubuntu Pro	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:canonical:ubuntu:22.10:*:*:*:*:*:*:*	-
XStream Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1203: Exploitation for Client Execution	https://www.vmware.com/security/advisories/VMSA-2022-0027.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2022-41328]()	✗	FortiOS: 6.4.0 - 6.4.11, 6.2.0 - 6.2.13, 6.0.0 - 6.0.16, 7.0.0 - 7.0.9, 7.2.0 - 7.2.3	UNC3886
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	-
Fortinet FortiOS Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059.006: Command and Scripting Interpreter: Python	https://www.fortiguard.com/psirt/FG-IR-22-369

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-24880	✗	Windows: 10 - 11 22H2 Windows Server: 2016 - 2022 20H2	-
	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	T1203: Exploitation for Client Execution	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-24880

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-23397	✗	Microsoft Outlook: 2013 - 2021 Microsoft Office: 365 - 2021	Unknown Russian threat actor
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:microsoft_outlook:2016:*:*:*:*:*:*:*	-
Microsoft Office Outlook Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1068: Exploitation for Privilege Escalation	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-23397

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26360	✗	ColdFusion: 2016 - 2021 Update 5	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:coldfusion:2021:Update 5:*:*:*:*:*:*	-
Adobe ColdFusion Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1203: Exploitation for Client Execution	https://coldfusion.adobe.com/2023/03/released-coldfusion-2021-and-2018-march-2023-security-updates/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2013-3163	✗	Microsoft Internet Explorer: 7 - 9	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:microsoft_internet_explorer:9:*:*:*:*:*:*:*	-
Microsoft Internet Explorer Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1203: Exploitation for Client Execution T1499: Endpoint Denial of Service	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-055

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-1776	✗	Microsoft Internet Explorer: 6 - 11	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:microsoft_internet_explorer:11:*:*:*:*:*:*:*	-
Microsoft Internet Explorer Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1203: Exploitation for Client Execution T1499: Endpoint Denial of Service	https://technet.microsoft.com/library/security/2963983

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-7494	SAMBA CRY	Gentoo Linux: All versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:gentoo:gentoo_linux:*:*:*:*:*:*:*:*	-
Samba Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-426	T1203: Exploitation for Client Execution	https://www.samba.org/samba/security/CVE-2017-7494.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-42948	✗	Fortra Cobalt Strike	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:helpsystems:cobalt_strike:4.7.1:*:*:*:*:*:*:*	-
Fortra Cobalt Strike User Interface Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1203: Exploitation for Client Execution	https://www.cobaltstrike.com/blog/out-of-band-update-cobalt-strike-4-7-2/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-39197	✗	Fortra Cobalt Strike	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:helpsystems:cobalt_strike:*:*:*:*:*:*:*:*	-
Fortra Cobalt Strike Teamserver Cross-Site Scripting (XSS) Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1189: Drive-By Compromise	https://www.cobaltstrike.com/blog/out-of-band-update-cobalt-strike-4-7-1/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-30900	✗	iPadOS: 14.0 18A373 - 14.8 18H17 Apple iOS: 14.8 18H17, 14.7 18G69 - 14.7.1 18G82, 14.5 18E199 - 14.5.1 18E212, 14.2 18B92 - 14.2.1 18B121, 14.0 18A373 - 14.0.1 18A393, 14.4 18D52 - 14.4.2 18D70	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:14.8:18H17:*:*:*:*:*:*	-
Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1404: Exploitation for Privilege Escalation	https://support.apple.com/en-us/HT212867 https://support.apple.com/en-us/HT212868 https://support.apple.com/kb/HT212872

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-38181	✗	Midgard GPU Kernel Driver: All versions Bifrost GPU Kernel Driver: before r40p0 Valhall GPU Kernel Driver: before r40p0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:arm:midgard_gpu_kernel_driver:*:*:*:*:*:*:*:*	-
Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1027: Obfuscated Files or Information	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-0266	✗	Linux Kernel	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:suse:suse_linux_enterprise_micro:5.4:*:*:*:*:*:*:*	-
Linux Kernel Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation	https://github.com/torvalds/linux/commit/56b88b50565cd8b946a2d00b0c83927b7ebb055e

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-3038	✗	Chrome OS: before 102.0.5005.189	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:chrome_os:*:*:*:*:*:*:*:	-
Google Chrome Use-After-Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1553.005: Subvert Trust Controls: Mark-of-the-Web Bypass	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_30.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-22706	✗	Midgard GPU Kernel Driver: before r32p0 Bifrost GPU Kernel Driver: before r36p0 Valhall GPU Kernel Driver: before r36p0	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:arm:bifrost:*:*:*:*:*:*:*:*	-
Arm Mali GPU Kernel Driver Unspecified Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities

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 Cybersecurity 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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

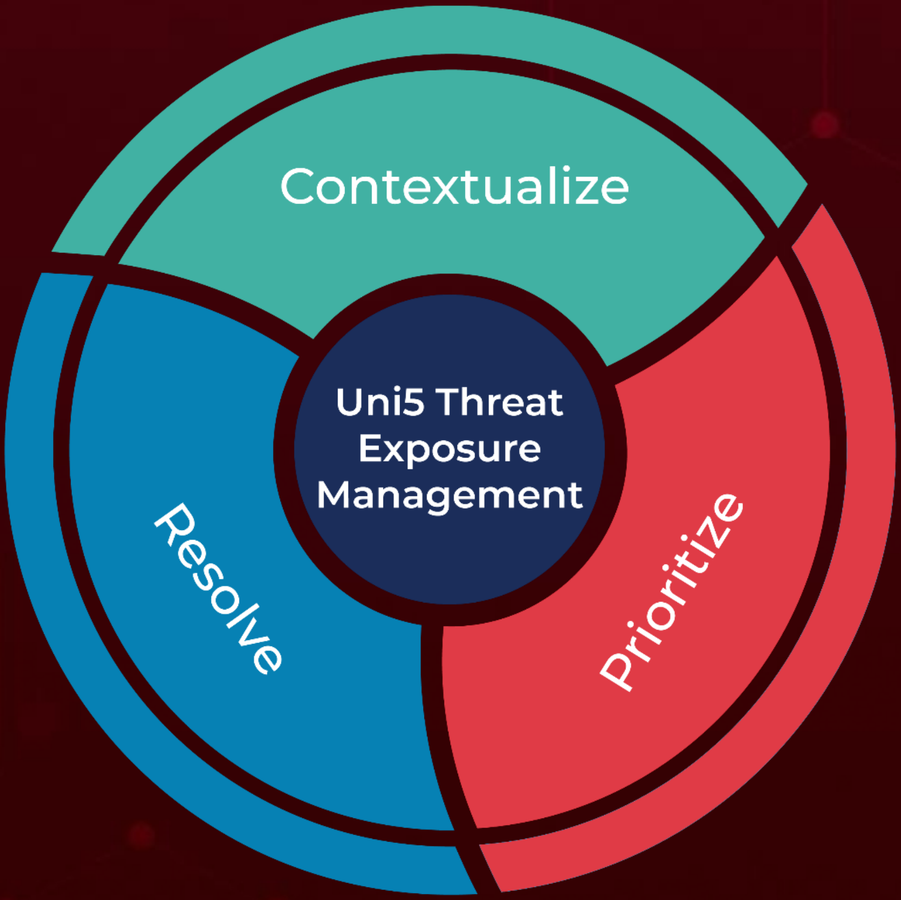
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

April 01, 2023 • 5:00 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com