Date of Publication
September 1, 2023

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

August 2023

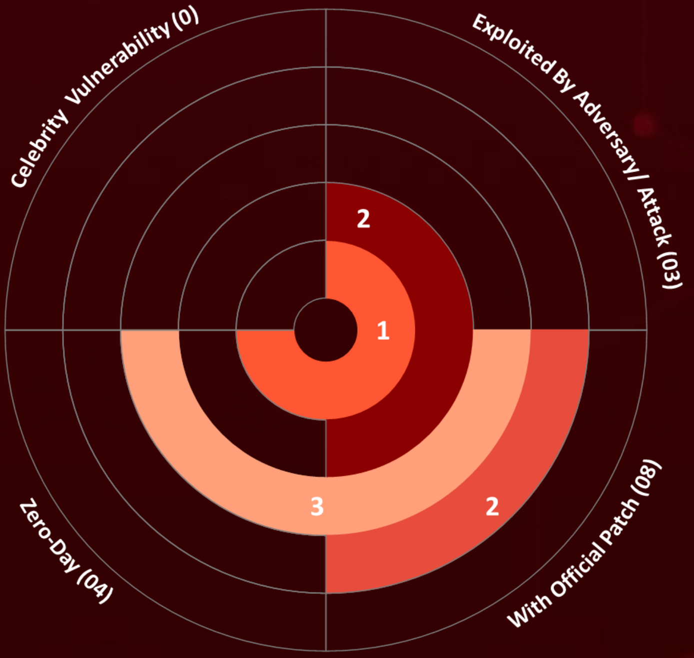
Table of Contents

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

8
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-38831	RARLAB WinRAR Code Execution Vulnerability	RARLAB WinRAR	7.8	✓	✓	September 14, 2023
CVE-2023-32315	Ignite Realtime Openfire Path Traversal Vulnerability	Ignite Realtime Openfire	7.5	✗	✓	September 14, 2023
CVE-2023-38035	Ivanti Sentry Authentication Bypass Vulnerability	Ivanti Sentry	9.8	✓	✓	September 12, 2023
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication	7.5	✗	✓	September 12, 2023
CVE-2023-26359	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	Adobe ColdFusion	9.8	✓	✓	September 11, 2023
CVE-2023-24489	Citrix Content Collaboration ShareFile Improper Access Control Vulnerability	Citrix Content Collaboration	9.8	✗	✓	September 6, 2023
CVE-2023-38180	Microsoft .NET Core and Visual Studio Denial-of-Service Vulnerability	Microsoft .NET Core and Visual Studio	7.5	✓	✓	August 30, 2023
CVE-2017-18368	Zyxel P660HN-T1A Routers Command Injection Vulnerability	Zyxel P660HN-T1A Routers	9.8	✗	✓	August 28, 2023

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831	✗	WinRAR version 6.22 and older versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:rarlab:winrar: 6.23:beta 1:*:*:*:*:*:*	DarkMe, GuLoader, and Remcos RAT
RARLAB WinRAR Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	http://www.win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32315	✗	Openfire versions: 3.10.0-4.7.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:igniterealtime:openfire:*:*:*:*:*:*:*:*	-
Ignite Realtime Openfire Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1202: Indirect Command Execution, T1632: Subvert Trust Controls	Upgrade Openfire versions to 4.6.8, 4.7.5, 4.8.0 or newer versions https://github.com/igniterealtime/Openfire/security/advisories/GHSA-gw42-f939-fhvm

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38035	✗	Ivanti Sentry versions 9.18. 9.17, 9.16 and older versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:mobileiron_sentry:*:*:*:*:*:*:*:*	-
Ivanti Sentry Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1040: Network Sniffing, T1078: Valid Accounts	https://forums.ivanti.com/s/article/KB-API-Authentication-Bypass-on-Sentry-Administrator-Interface-CVE-2023-38035

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27532	✗	Veeam Backup & Replication, Veeam Cloud Connect, Veeam Cloud Connect for the Enterprise & Veeam Backup & Replication Community Edition	FIN7
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:veeam:backup_\&_replication:11.0.1.1261:*:*:*:*:*:*:*	Cuba ransomware, BURNTCIGAR, POWERTRASH Loader & DICELOADER
Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1040: Network Sniffing, T1574: Hijack Execution Flow	https://www.veeam.com/kb4424

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26359	✗	Adobe ColdFusion: 2018 & 2021	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:coldfusion:2021:Update5:*:*:*:*:*:*	-
Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://coldfusion.adobe.com/2023/03/released-coldfusion-2021-and-2018-march-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-24489	✗	Citrix Content Collaboration before version 5.11.24.	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:citrix:sharefile_storage_zones_controller:*:*:*:*:*:*:*:*	-
Citrix Content Collaboration ShareFile Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1632: Subvert Trust Controls, T1562: Impair Defenses	https://support.citrix.com/article/CTX559517/sharefile-storagezones-controller-security-update-for-cve202324489

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38180	✗	.NET: 6.0.0 - 7.0.9, Visual Studio: 17.2.0 17.2.32505.173 - 17.6.5 17.6.33829.357, ASP.NET Core: before 2.1.40	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:.net:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:visual_studio_2022:*:*:*:*:*:*:*:*	-
Microsoft .NET Core and Visual Studio Denial-of-Service Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1499.004: Application or System Exploitation, T1574: Hijack Execution Flow	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-18368	✗	Zyxel P660HN-T1A Routers	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:zyxel:p660hn-t1a_v2:-:*:*:*:*:*:*:*	Gafgyt botnet
Zyxel P660HN-T1A Routers Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/zyxel-security-advisory-for-a-new-variant-of-gafgyt-malware https://www.zyxel.com/global/en/support/zyxel-security-advisory-for-command-injection-vulnerability-in-p660hn-t1a-dsl-cpe

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 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.

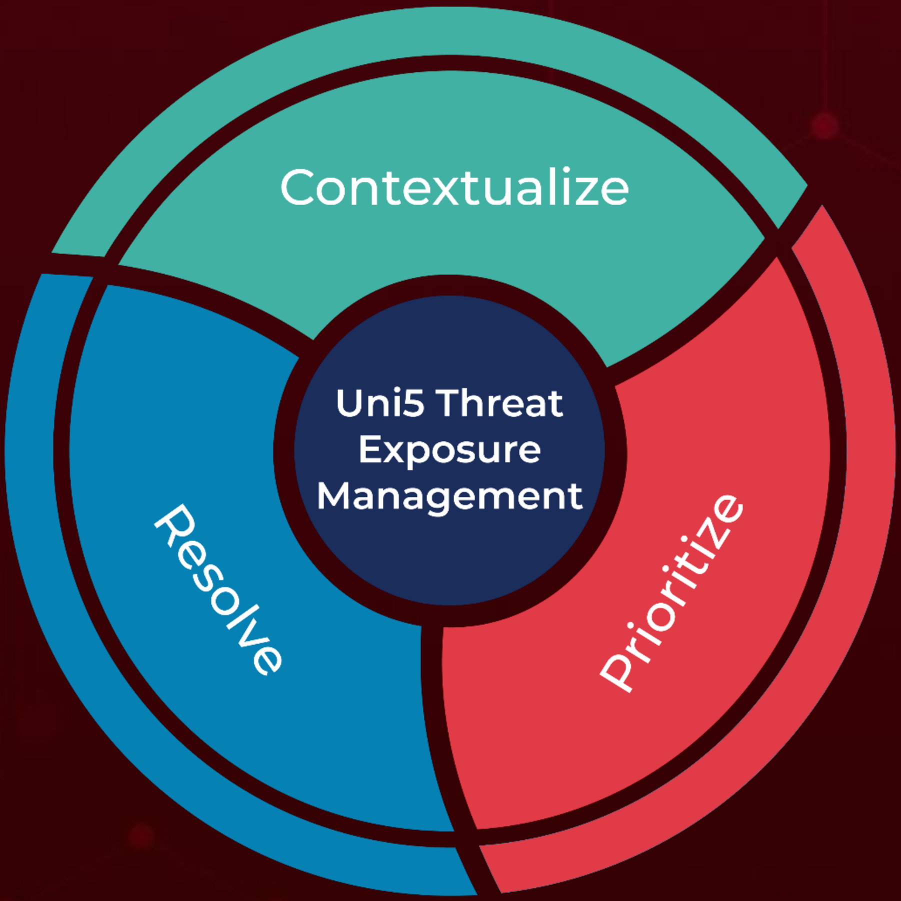
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

September 1, 2023 • 3:00 AM

More at www.hivepro.com