



HiveForce Labs

**CISA**

**KNOWN**

**EXPLOITED**

**VULNERABILITY**

**CATALOG**

**April 2023**

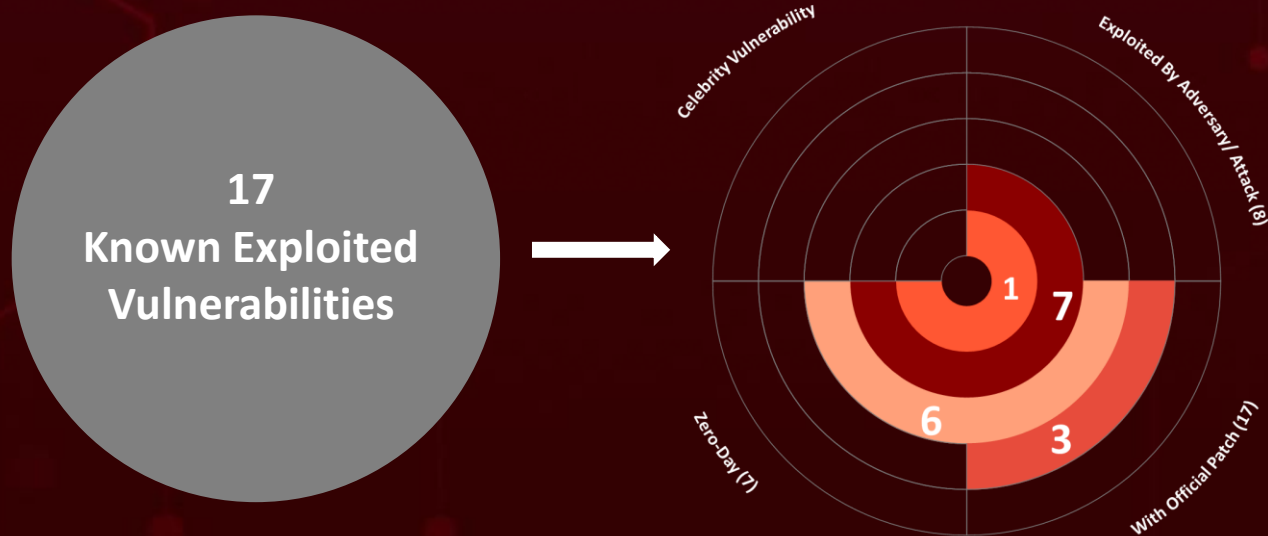
# Table of Contents

<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	06
<u>Recommendations</u>	15
<u>References</u>	16
<u>Appendix</u>	16
<u>What Next?</u>	17

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











# CVEs List




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2022-27926	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	Zimbra Collaboration (ZCS)	6.1			April 24, 2023
CVE-2021-27876	Veritas Backup Exec Agent File Access Vulnerability	Veritas Backup Exec Agent	8.1			April 28, 2023
CVE-2021-27877	Veritas Backup Exec Agent Improper Authentication Vulnerability	Veritas Backup Exec Agent	8.2			April 28, 2023
CVE-2021-27878	Veritas Backup Exec Agent Command Execution Vulnerability	Veritas Backup Exec Agent	8.8			April 28, 2023
CVE-2019-1388	Microsoft Windows Certificate Dialog Privilege Escalation Vulnerability	Microsoft Windows	7.8			April 28, 2023
CVE-2023-26083	Arm Mali GPU Kernel Driver Information Disclosure Vulnerability	Arm Mali Graphics Processing Unit (GPU)	3.3			April 28, 2023
CVE-2023-28205	Apple Multiple Products WebKit Use-After-Free Vulnerability	Apple Multiple Products	8.8			May 1, 2023
CVE-2023-28206	Apple iOS, iPadOS, and macOS IOSurfaceAccelerator Out-of-Bounds Write Vulnerability	Apple iOS, iPadOS, and macOS	8.6			May 1, 2023
CVE-2023-28252	Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability	Microsoft Windows	7.8			May 2, 2023
CVE-2023-20963	Android Framework Privilege Escalation Vulnerability	Android Framework	7.8			May 4, 2023




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-29492	Novi Survey Insecure Deserialization Vulnerability	Novi Survey	9.8			May 4, 2023
CVE-2019-8526	Apple macOS Use-After-Free Vulnerability	Apple macOS	7.8			May 8, 2023
CVE-2023-2033	Google Chromium V8 Engine Type Confusion Vulnerability	Google Chromium V8 Engine	8.8			May 8, 2023
CVE-2017-6742	Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability	Cisco IOS and IOS XE Software	8.8			May 10, 2023
CVE-2023-28432	MinIO Information Disclosure Vulnerability	MinIO	7.5			May 12, 2023
CVE-2023-27350	PaperCut MF/NG Improper Access Control Vulnerability	PaperCut MF/NG	9.8			May 12, 2023
CVE-2023-2136	Google Chrome Skia Integer Overflow Vulnerability	Google Chrome	9.6			May 12, 2023

# CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-27926</u>		Zimbra Collaboration: 9.0.0 P23	Winter Vivern (aka TA473 and UAC-0114)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:zimbra:collaboration:9.0.0:-:*:*:*:*:*	-
Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1189: Drive-By Compromise	<a href="https://wiki.zimbra.com/wiki/Security_Center">https://wiki.zimbra.com/wiki/Security_Center</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-27876</u>		Backup Exec: 16 FP1 (16.0.1142.1327) - 21.1	UNC4466
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:veritas:backup_exec:*:*:*:*:*:*:*	BlackCat(aka ALPHV and Noberus) ransomware
Veritas Backup Exec Agent File Access Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1078: Valid Accounts	<a href="https://www.veritas.com/support/en_US/security/VTS21-001">https://www.veritas.com/support/en_US/security/VTS21-001</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-27877</u>		Backup Exec: 16 FP1 (16.0.1142.1327) - 21.1	UNC4466
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:veritas:backup_exec:*:*:*:*:*:*	BlackCat(aka ALPHV and Noberus) ransomware
Veritas Backup Exec Agent Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1078: Valid Accounts	<a href="https://www.veritas.com/support/en_US/security/VTS21-001">https://www.veritas.com/support/en_US/security/VTS21-001</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-27878</u>		Backup Exec: 16 FP1 (16.0.1142.1327) - 21.1	UNC4466
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:veritas:backup_exec:*:*:*:*:*:*	BlackCat(aka ALPHV and Noberus) ransomware
Veritas Backup Exec Agent Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1078: Valid Accounts	<a href="https://www.veritas.com/support/en_US/security/VTS21-001">https://www.veritas.com/support/en_US/security/VTS21-001</a>














CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28205		Apple Safari: 16.0 - 16.4, iPadOS: 15.0 19A346 - 15.7.4 19H321, Apple iOS: 15.0 19A346 - 15.7.4 19H321, & macOS: 13.0 22A380 - 13.3 22E252	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apple:safari:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*	-
Apple Multiple Products WebKit Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1553:Subvert Trust Controls; T1553.005:Mark-of-the-Web Bypass	<a href="https://support.apple.com/en-us/HT213720">https://support.apple.com/en-us/HT213720</a> , <a href="https://support.apple.com/en-us/HT213721">https://support.apple.com/en-us/HT213721</a> , <a href="https://support.apple.com/en-us/HT213722">https://support.apple.com/en-us/HT213722</a> , <a href="https://support.apple.com/en-us/HT213723">https://support.apple.com/en-us/HT213723</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28206		macOS: 13.0 22A380 - 13.3 22E252	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipad os:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:* *	-
Apple iOS, iPadOS, and macOS IOSurfaceAccelerator Out-of-Bounds Write Vulnerability		cpe:2.3:o:apple:macos:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation	<a href="https://support.apple.com/en-us/HT213720">https://support.apple.com/en-us/HT213720</a> , <a href="https://support.apple.com/en-us/HT213721">https://support.apple.com/en-us/HT213721</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28252		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:*:*:*:*:*:* :*:* cpe:2.3:o:microsoft:windows_server:- :*:*:*:*:*:*"	Nokoyawa Ransomware
Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	
	CWE-119	T1203: Exploitation for Client Execution; T1499: Endpoint Denial of Service	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28252">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28252</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20963		Google Android: 13 - 13 2023-02-05, 12 - 12L 2023-02-05, 11 - 11 2023-02-05	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:-:*:*:*:*:*	-
Android Framework Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-295	T1068:Exploitation for Privilege Escalation;T1204: User Execution; T1204.001:Malicious Link	<a href="https://source.android.com/docs/security/bulletin/2023-03-01">https://source.android.com/docs/security/bulletin/2023-03-01</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29492		Novi Survey before 8.9.43676	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:novisurvey:novi_survey:*:*:*:*:*.*.*.*.*	-
Novi Survey Insecure Deserialization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1203: Exploitation for Client Execution	<a href="https://novisurvey.net/blog/novi-survey-security-advisory-apr-2023.aspx">https://novisurvey.net/blog/novi-survey-security-advisory-apr-2023.aspx</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2019-8526</u>		macOS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*	DazzleSpy Backdoor
Apple macOS Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1203: Exploitation for Client Execution; T1499: Endpoint Denial of Service	<a href="https://support.apple.com/en-us/HT209600">https://support.apple.com/en-us/HT209600</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-2033</u>		Google Chrome: All versions (before 112.0.5615.121)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
Google Chromium V8 Engine Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1562:Impair Defenses; T1005:Data from Local System	<a href="https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_14.html">https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_14.html</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2017-6742</u>		Cisco IOS: 15.6.3 M1 - 16.5.1 & Cisco IOS XE: 3.16.1aS	APT28(Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium , Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12 , ITG05, TAG-0700, UAC-0028, Grey-Cloud)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:ios_xe:-:*:*:*:*:*:*	-
Cisco IOS and IOS XE Software SNMP Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1203: Exploitation for Client Execution; T1499: Endpoint Denial of Service	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-28432</u>		minio: 2019-12-17T23:16:33Z - 2023-03-13T19:46:17Z	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:minio:minio:*:*:*:*:*:*	-
MinIO Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1078:Valid Accounts;T1040:Network Sniffing	<a href="https://github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q">https://github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-27350</u>		PaperCutMF: before 22.0.9	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*	Clon ransomware and Truebot
PaperCut MF/NG Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1478:Install Insecure or Malicious Configuration	<a href="https://www.papercut.com/kb/Main/PO-1216-and-PO-1219">https://www.papercut.com/kb/Main/PO-1216-and-PO-1219</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-2136</u>		Google Chrome: 100.0.4896.60 - 112.0.5615.121	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
Google Chrome Skia Integer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1574:Hijack Execution Flow; T1499:Endpoint Denial of Service; T1499.004:Application or System Exploitation;T1548:Abuse Elevation Control Mechanism; T1548.001:Setuid and Setgid	<a href="https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html">https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_18.html</a>

# 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.

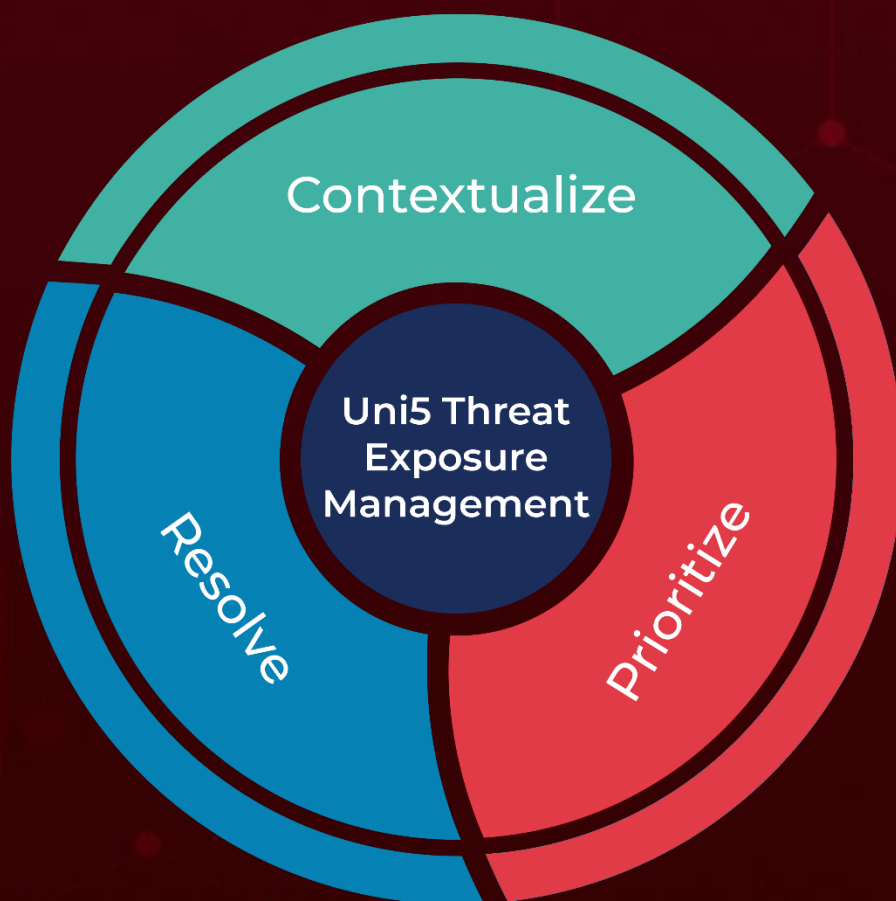
**Due Date:** The "Due Date" provided by CISA is a recommended deadline that organizations should use to prioritize the remediation of identified vulnerabilities in their systems, with the aim of enhancing their overall security posture.



# 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

**May 3, 2023 • 5:55 AM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)