

Date of Publication  
March 1, 2024



HiveForce Labs

**CISA**

**KNOWN**

**EXPLOITED**

**VULNERABILITY**

**CATALOG**

**February 2024**

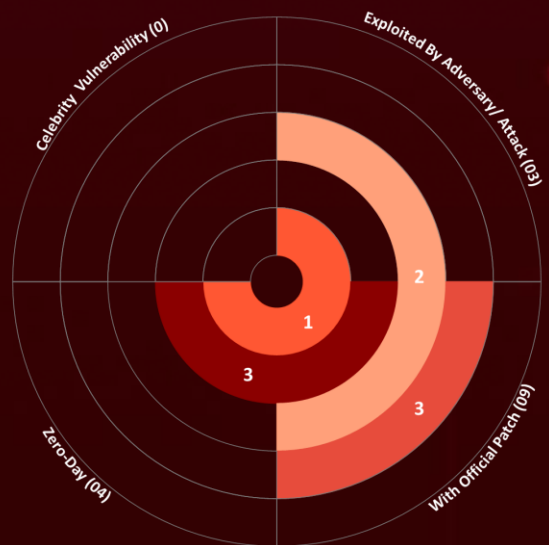
# Table of Contents

<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	05
<u>Recommendations</u>	10
<u>References</u>	11
<u>Appendix</u>	11
<u>What Next?</u>	12

# 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 February 2024, Nine 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.














# CVEs List




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-4762	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8	8.8			February 27, 2024
CVE-2024-21762	Fortinet FortiOS Out-of-Bound Write Vulnerability	Fortinet FortiOS	9.8			February 16, 2024
CVE-2023-43770	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	Roundcube Webmail	6.1			March 4, 2024
CVE-2024-21412	Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability	Microsoft Windows	8.1			March 5, 2024
CVE-2024-21351	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	7.6			March 5, 2024
CVE-2020-3259	Cisco ASA and FTD Information Disclosure Vulnerability	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	7.5			March 7, 2024
CVE-2024-21410	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server	9.8			March 7, 2024
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	10.0			February 29, 2024
CVE-2023-29360	Microsoft Streaming Service Untrusted Pointer Dereference Vulnerability	Microsoft Streaming Service	8.4			March 21, 2024




# CVEs Details




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4762		Google Chrome prior to 116.0.5845.179	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*	-
Google Chromium V8 Type Confusion Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter, T1189 : Drive-by Compromise	<a href="https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop.html">https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop.html</a>
	CWE-843		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21762		Fortinet FortiOS versions: 7.4.0 through 7.4.2 7.2.0 through 7.2.6 7.0.0 through 7.0.13 6.4.0 through 6.4.14 6.2.0 through 6.2.15 6.0 all versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*	-
Fortinet FortiOS Out-of-Bound Write Vulnerability			
	CWE ID	T1203 : Exploitation for Client Execution	<a href="https://fortiguard.fortinet.com/psirt/FG-IR-24-015">https://fortiguard.fortinet.com/psirt/FG-IR-24-015</a>
	CWE-787		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2023-43770</a>		Roundcube before 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*	-
Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059 : Command and Scripting Interpreter, T1204 : User Execution	<a href="https://roundcube.net/news/2023/09/15/security-update-1.6.3-released">https://roundcube.net/news/2023/09/15/security-update-1.6.3-released</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#">CVE-2024-21412</a>		Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	Water Hydra
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1204.001 User Execution: Malicious Link, T1036.008 Masquerading: Masquerade File Type	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21412">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21412</a>




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-21351</u></a>		Windows: 10 - 11 23H2 Windows Server: 2016 – 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 SmartScreen Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-254	T1204.002 User Execution: Malicious File, T1553.005 Subvert Trust Controls: Mark-of-the-Web Bypass	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21351">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21351</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2020-3259</u></a>		Cisco ASA and FTD	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*	Akira Ransomware
Cisco ASA and FTD Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-200	1190 : Exploit Public-Facing Application, T1082 : System Information Discovery	<a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-21410</u></a>		Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:exchange_server:2016:cu23:*:*:*:*:*:*	-
Microsoft Exchange Server Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-668	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21410">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21410</a>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<a href="#"><u>CVE-2024-1709</u></a>		ScreenConnect 23.9.7 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS		LockBit Ransomware, BlackBasta Ransomware, Bl00dy Ransomware, Blackcat Ransomware, XWORM, and AsyncRAT
ConnectWise ScreenConnect Authentication Bypass Vulnerability		cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190 : Exploit Public-Facing Application, T1136 : Create Account	<a href="https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8">https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8</a>



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29360		Microsoft Exchange Server: 2016 CU22 Nov22SU 15.01.2375.037 - 2019 RTM Mar21SU 15.02.0221.018	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_10_1607:*:*:*:*:*:x64:*	-
Microsoft Streaming Service Untrusted Pointer Dereference Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-668	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29360">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29360</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 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.

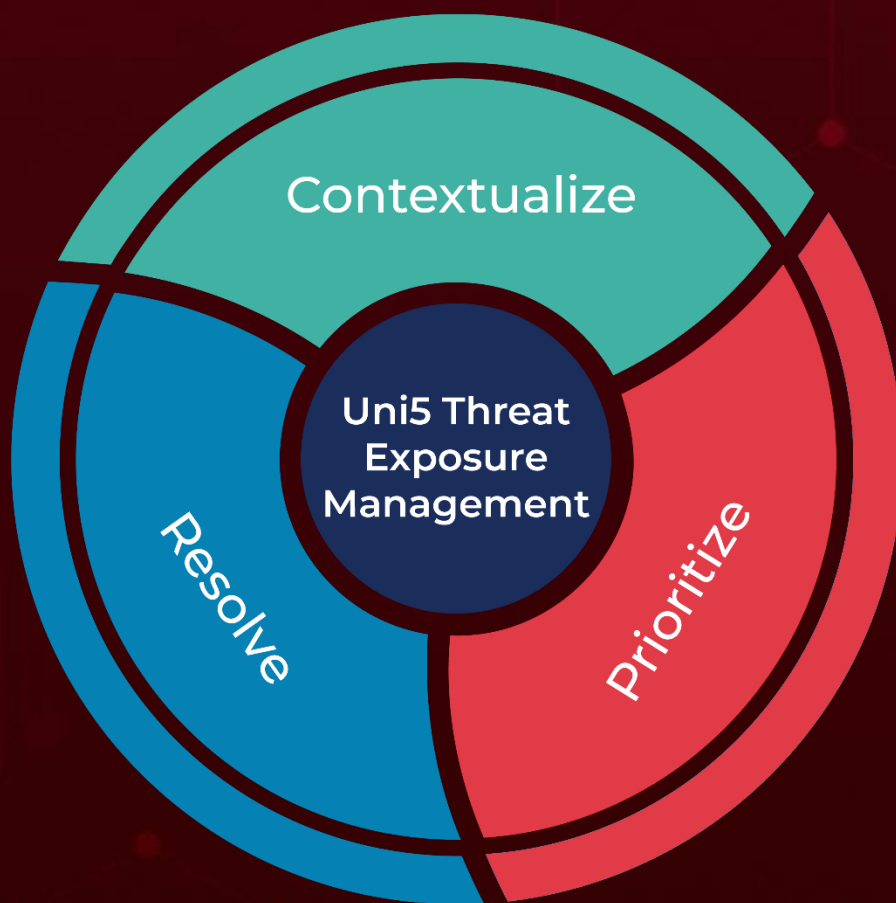
**BAS Attacks:** “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

**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

**March 1, 2024 • 3:30 AM**

© 2024 All Rights are Reserved by Hive Pro®



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