

Date of Publication
April 3, 2024



HiveForce Labs

CISA

KNOWN

EXPLOITED

VULNERABILITY

CATALOG

March 2024

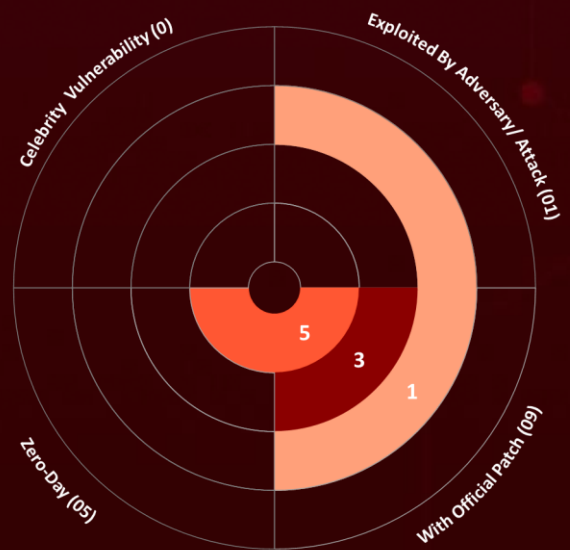
Table of Contents

<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	06
<u>Recommendations</u>	12
<u>References</u>	13
<u>Appendix</u>	13
<u>What Next?</u>	14

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 2024, Ten vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, five are zero-day vulnerabilities; one 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-2024-21338	Microsoft Windows Kernel Exposed IOCTL with Insufficient Access Control Vulnerability	Windows	7.8			March 25, 2024
CVE-2023-21237	Android Pixel Information Disclosure Vulnerability	Pixel	5.5			March 26, 2024
CVE-2021-36380	Sunhillo SureLine OS Command Injection Vulnerability	SureLine	9.8			March 26, 2024
CVE-2024-23225	Apple Multiple Products Memory Corruption Vulnerability	Multiple Products	7.8			March 27, 2024
CVE-2024-23296	Apple Multiple Products Memory Corruption Vulnerability	Multiple Products	7.8			March 27, 2024
CVE-2024-27198	JetBrains TeamCity Authentication Bypass Vulnerability	TeamCity	9.8			March 28, 2024
CVE-2019-7256	Nice Linear eMerge E3-Series OS Command Injection Vulnerability	Linear eMerge E3-Series	10.0			April 15, 2024
CVE-2021-44529	Ivanti Endpoint Manager Cloud Service Appliance (EPM CSA) Code Injection Vulnerability	Endpoint Manager Cloud Service Appliance (EPM CSA)	9.8			April 15, 2024




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-48788	Fortinet FortiClient EMS SQL Injection Vulnerability	FortiClient EMS	9.8			April 15, 2024
CVE-2023-24955	Microsoft SharePoint Server Code Injection Vulnerability	SharePoint Server	7.2			April 16, 2024




CVEs Details




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21338		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:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
Microsoft Windows Kernel Exposed IOCTL with Insufficient Access Control Vulnerability		T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21338
	CWE ID		
	CWE-264		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-21237		Pixel: before 2023-06-05	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:13.0:*:*:*:*:*:*	-
Android Pixel Information Disclosure Vulnerability		T1426: System Information Discovery	https://source.android.com/docs/security/bulletin/pixel/2023-06-01#Security-patches
	CWE ID		
	CWE-200		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-36380		SureLine: 8.7.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sunhillo:sureline :*:*:*:*:*:*:*	-
Sunhillo SureLine OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.sunhillo.com/product/sureline/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23225		Apple iOS, iPadOS, macOS, tvOS, watchOS, and visionOS kernel	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipad_os:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*	-
Apple Multiple Products Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1211 : Exploitation for Defense Evasion, T1106 : Native API	https://support.apple.com/en-us/HT214081 ; https://support.apple.com/en-us/HT214082




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-23296</u>		Apple iOS, iPadOS, macOS, tvOS, watchOS, and visionOS kernel	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSO MWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipad_os:*:*:*:*:*:* *.*	
Apple Multiple Products Memory Corruption Vulnerability		cpe:2.3:o:apple:iphone_os:*:*:*:*:* *.*.*.* cpe:2.3:o:apple:macos:*:*:*:*:*:* .* cpe:2.3:o:apple:tvos:*:*:*:*:*.* cpe:2.3:o:apple:visionos:*:*:*:*:*.* .*.* cpe:2.3:o:apple:watchos:*:*:*:*:*.* .*.*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1211 : Exploitation for Defense Evasion, T1106 : Native API	https://support.apple.com/en-us/HT214081 ; https://support.apple.com/en-us/HT214082

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27198		TeamCity On-Premises versions upto 2023.11.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*	Jasmin ransomware, XMRig, SparkRAT backdoor
JetBrains TeamCity Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-288	T1556 : Modify Authentication Process, T1190 : Exploit Public-Facing Application	https://www.jetbrains.com/teamcity/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-7256		eMerge E3-Series: All versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:nortekcontrol:linear_emerge_essential_firmware:*:*:*:*:*:* cpe:2.3:h:nortekcontrol:linear_emerge_essential:*:*:*:*:*:*	-
Nice Linear eMerge E3-Series OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44529		CSA 4.6 4.5 - EOF Aug 2021	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*	-
Ivanti Endpoint Manager Cloud Service Appliance (EPM CSA) Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://forums.ivanti.com/s/article/SA-2021-12-02

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-48788		FortiClientEMS 7.2.0 through 7.2.2 FortiClientEMS 7.0.1 through 7.0.10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:forticlient_enterprise_management_server:*:*:*:*:*:*	-
Fortinet FortiClient EMS SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-89	T1055: Process Injection	https://fortiguard.fortinet.com/psirt/FG-IR-24-007

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-24955</u>		Microsoft SharePoint Server: 2016, 2019, Subscription Edition All versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint_enterprise_server:2016:*:*:*:*:*:* cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*:subscription:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*	-
Microsoft SharePoint Server Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955

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.

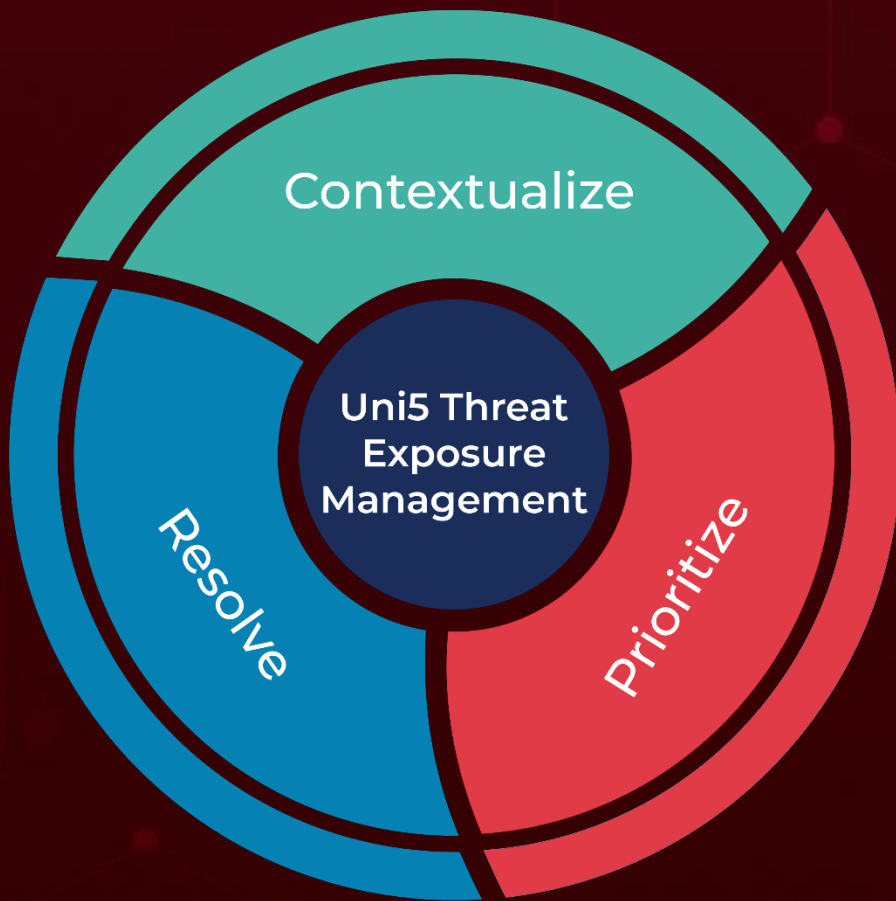
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

April 3, 2024 • 5:20 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com