

Date of Publication
November 1, 2023



HiveForce Labs

CISA

KNOWN

EXPLOITED

VULNERABILITY

CATALOG

October 2023

Table of Contents

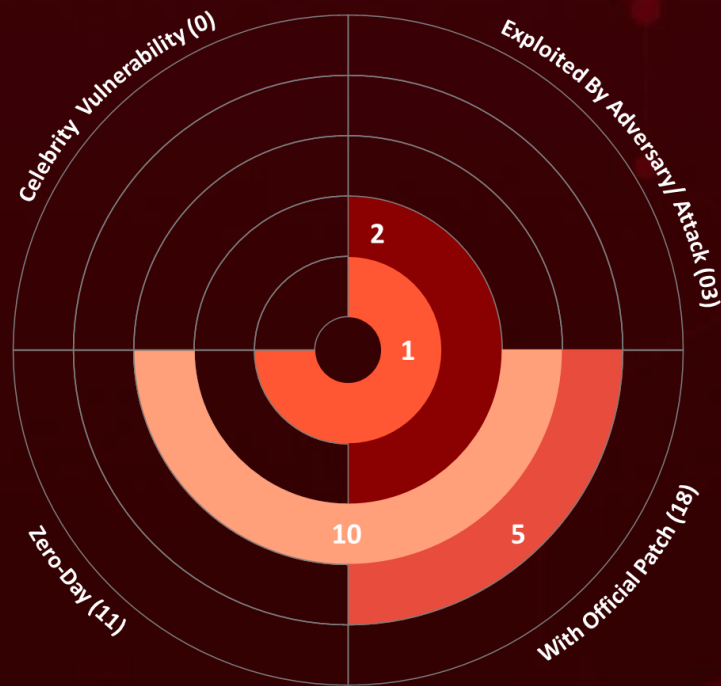
<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	06
<u>Recommendations</u>	15
<u>References</u>	16
<u>Appendix</u>	16
<u>What Next?</u>	17

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

18
Known Exploited
Vulnerabilities











CVEs List




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-46748	F5 BIG-IP Configuration Utility SQL Injection Vulnerability	F5 BIG-IP Configuration Utility	8.8			November 21, 2023
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration Utility	9.8			November 21, 2023
CVE-2023-5631	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	Roundcube Webmail	5.4			November 16, 2023
CVE-2023-20273	Cisco IOS XE Web UI Command Injection Vulnerability	Cisco Cisco IOS XE Web UI	7.2			October 27, 2023
CVE-2023-4966	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	7.5			November 8, 2023
CVE-2023-20198	Cisco IOS XE Web UI Privilege Escalation Vulnerability	Cisco IOS XE Web UI	10			October 20, 2023
CVE-2023-21608	Adobe Acrobat and Reader Use-After-Free Vulnerability	Adobe Acrobat and Reader	7.8			October 31, 2023
CVE-2023-20109	Cisco IOS and IOS XE Group Encrypted Transport VPN Out-of-Bounds Write Vulnerability	Cisco IOS and IOS XE	6.6			October 31, 2023
CVE-2023-41763	Microsoft Skype for Business Privilege Escalation Vulnerability	Microsoft Skype for Business	5.3			October 31, 2023
CVE-2023-36563	Microsoft WordPad Information Disclosure Vulnerability	Microsoft WordPad	6.5			October 31, 2023




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-44487	HTTP/2 Rapid Reset Attack Vulnerability	IETF HTTP/2	7.5			October 31, 2023
CVE-2023-22515	Atlassian Confluence Data Center and Server Broken Access Control Vulnerability	Atlassian Confluence Data Center and Server	9.8			October 13, 2023
CVE-2023-40044	Progress WS_FTP Server Deserialization of Untrusted Data Vulnerability	Progress WS_FTP Server	8.8			October 26, 2023
CVE-2023-42824	Apple iOS and iPadOS Kernel Privilege Escalation Vulnerability	Apple iOS and iPadOS	7.8			October 26, 2023
CVE-2023-42793	JetBrains TeamCity Authentication Bypass Vulnerability	JetBrains TeamCity	9.8			October 25, 2023
CVE-2023-28229	Microsoft Windows CNG Key Isolation Service Privilege Escalation Vulnerability	Microsoft Windows CNG Key Isolation Service	7			October 25, 2023
CVE-2023-4211	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	Arm Mali GPU Kernel Driver	5.5			October 24, 2023
CVE-2023-5217	Google Chrome libvpx Heap Buffer Overflow Vulnerability	Google Chrome libvpx	8.8			October 23, 2023




CVEs Details




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46748		BIG-IP: 13.1.0 - 17.1.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:f5_networks:big-ip:- .*:.*:.*:.*:.*	-
F5 BIG-IP Configuration Utility SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1505.003: Web Shell, T1136: Create Account, T1190: Exploit Public-Facing Application, T1565.001: Stored Data Manipulation	https://my.f5.com/manage/s/article/K000137365




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46747		BIG-IP: 13.1.0 - 17.1.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:f5_networks:big-ip:- .*:.*:.*:.*:.*	-
F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-288	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://my.f5.com/manage/s/article/K000137353




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-5631</u>		Roundcube: 1.0.0 - 1.6.3	Winter Vivern
	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	T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1557: Adversary-in-the-Browser, T1189: Drive-by Compromise, T1204.001: User Execution	https://roundcube.net/news/2023/10/16/security-update-1.6.4-released , https://roundcube.net/news/2023/10/16/security-updates-1.5.5-and-1.4.15
	CWE-79		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-20273</u>		Cisco IOS XE: before 17.9.4a	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:ios_xe:*:*:*:*:*:*	-
Cisco IOS XE Web UI Command Injection Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
	CWE-269		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4966		Citrix Netscaler ADC: 12.1-55.289 - 14.1-4.42 & Citrix NetScaler Gateway: 12.1-55.289 - 14.1-4.42	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1574: Hijack Execution Flow, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20198		Cisco IOS XE: before 17.9.4a	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:ios_xe:*:*:*:*:*	-
Cisco IOS XE Web UI Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/CiscoSecurityAdvisory/cisco-sa-iosxe




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-21608		Adobe Acrobat: 20.001.30002 - 22.003.20282 & Adobe Reader: 20.005.30331 - 22.003.20282	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:acrobat_dc:*:*:*:continuous:*:*:* cpe:2.3:a:adobe:acrobat_reader_dc:*:*:*:continuous:*:*:*	-
Adobe Acrobat and Reader Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter	https://helpx.adobe.com/security/products/acrobat/apsb23-01.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20109		Cisco IOS: before 17.12.1 & Cisco IOS XE: before 17.12.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco_systems:cisco_ios:*:*:*:*:*:*	-
Cisco IOS and IOS XE Group Encrypted Transport VPN Out-of-Bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1565.001: Stored Data Manipulation, T1059: Command and Scripting Interpreter, T1574: Hijack Execution Flow, T1554: Compromise Client Software Binary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-getvpn-rce-g8qR68sx




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41763		Skype for Business Server: before 7.0.246.530	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:skype_for_business_server:*:*:*:*:*:*	-
Microsoft Skype for Business Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1068: Exploitation for Privilege Escalation, T1204: User Execution	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-41763




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36563		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:*:*:*:*:*:*	-
Microsoft WordPad Information Disclosure Vulnerability		cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1005: Data from Local System, T1078: Valid Accounts, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-36563




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-44487		Microsoft IIS: 10.0, Apache Tomcat: 8.5.0 -11.0.0-M11, Netty: 4.0.0 -4.1.99, Jetty: 9.0.0.v20130308 -12.0.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:iis:10.0:*:*:*:*:*	
HTTP/2 Rapid Reset Attack Vulnerability		cpe:2.3:a:apache_foundation:apache_tomcat:11.0.0-M11:*:*:*:*:* cpe:2.3:a:netty:netty:4.1.99:*:*:*:*:* cpe:2.3:a:eclipse:jetty:9.4.53.v20230927:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-400	T1588: Obtain Capabilities, T1498: Network Denial of Service, T1584: Compromise Infrastructure	https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22515		Confluence Server and Data Center: 8.0.0 - 8.5.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:atlassian:confluence_server_and_data_center:*:*:*:*:*	
Atlassian Confluence Data Center and Server Broken Access Control Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1588: Obtain Capabilities, T1548: Abuse Elevation Control Mechanism	https://confluence.atlassian.com/cve-2023-22515-privilege-escalation-vulnerability.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR	
CVE-2023-40044		WS_FTP: 7.0 - 8.8.1	-	
	ZERO-DAY			
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE	
NAME	BAS ATTACKS	cpe:2.3:a:progress:ws_ftp_server:*:*:*:*:*:*	-	
Progress WS_FTP Server Deserialization of Untrusted Data Vulnerability				CWE ID
	CWE-502	T1059: Command and Scripting Interpreter	https://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR	
CVE-2023-42824		iPadOS: 17.0 - 17.0.2, 16.0 20A362 - 16.7 & Apple iOS: 17.0 21A326 - 17.0.2 21A351, 16.0 20A362 - 16.7	-	
	ZERO-DAY			
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE	
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:* *:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:* *:*:*:*:*	-	
Apple iOS and iPadOS Kernel Privilege Escalation Vulnerability				CWE ID
	CWE-119	T1068: Exploitation for Privilege Escalation	https://support.apple.com/en-us/HT213961	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42793		TeamCity: 2023.05 - 2023.05.3	Lazarus Group & Andariel
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*	ForestTiger, FeedLoad, RollSling, HazyLoad
JetBrains TeamCity Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://blog.jetbrains.com/teamcity/2023/09/critical-security-issue-affecting-teamcity-on-premises-update-to-2023-05-4-now/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28229		Windows: 10 - 11 22H2 & Windows Server: 2008 – 2022	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Microsoft Windows CNG Key Isolation Service Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-362	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4211		Midgard GPU Kernel Driver: r12p0 - r32p0, Arm 5th Gen GPU Architecture Kernel Driver: r41p0 - r42p0, Valhall GPU Kernel Driver: before r43p0, Bifrost GPU Kernel Driver: before r43p0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:arm:valhall:*:*:*:*:*:* cpe:2.3:a:arm:midgard:*:*:*:*:*:* cpe:2.3:a:arm:bifrost:*:*:*:*:*:* cpe:2.3:a:arm:5th_gen_gpu_architecture_kernel_driver:*:*:*:*:*:*	-
Arm Mali GPU Kernel Driver Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter	https://developer.arm.com/Arm/Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-5217		Google Chrome:100.0.4896.60 - 117.0.5938.92,Firefox:100.0 - 118.0,Firefox ESR:10.0 -115.3.0, Firefox Focus for Android:108.2.0 - 118.0,66.0.4 -118.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:webmproject:libvpx:1.13.1:*:*:*:*:*	
Google Chrome libvpx Heap Buffer Overflow Vulnerability		cpe:2.3:a:google:chrome:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox:*:*:*:*:*:* *	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1574: Hijack Execution Flow, T1499.004: Application or System Exploitation	https://chromereleases.googleblog.com/2023/09.html

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 impact are profound and multifaceted. These vulnerabilities provide malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information. This is also known 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

November 1, 2023 • 10:00 PM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com