Date of Publication
June 1, 2023

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

May 2023

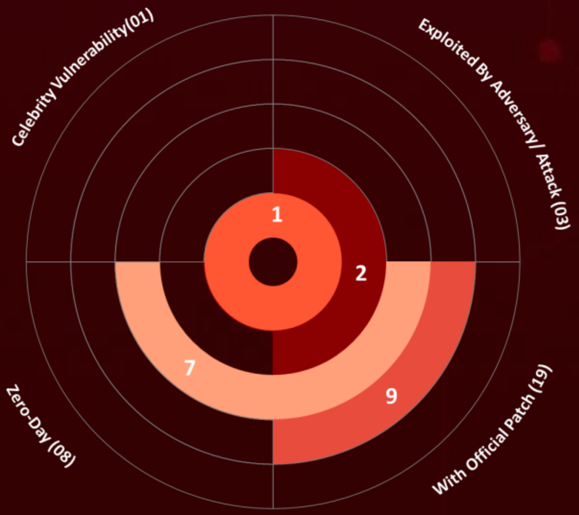
Table of Contents

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

19
Known Exploited
Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-1389	TP-Link Archer AX-21 Command Injection Vulnerability	TP-Link product	8.8	✗	✓	May 22, 2023
CVE-2021-45046	Apache Log4j2 Deserialization of Untrusted Data Vulnerability	Apache Archer AX21	9.0	✓	✓	May 22, 2023
CVE-2023-21839	Oracle WebLogic Server Unspecified Vulnerability	Oracle Log4j2	7.5	✗	✓	May 22, 2023
CVE-2023-29336	Microsoft Win32K Privilege Escalation Vulnerability	Microsoft WebLogic Server	7.8	✓	✓	May 30, 2023
CVE-2023-25717	Multiple Ruckus Wireless Products CSRF and RCE Vulnerability	Ruckus Wireless Win32k	9.8	✗	✓	June 2, 2023
CVE-2021-3560	Red Hat Polkit Incorrect Authorization Vulnerability	Red Hat Multiple Products	7.8	✗	✓	June 2, 2023
CVE-2014-0196	Linux Kernel Race Condition Vulnerability	Linux Polkit	6.9	✗	✓	June 2, 2023
CVE-2010-3904	Linux Kernel Improper Input Validation Vulnerability	Linux Kernel	7.2	✗	✓	June 2, 2023
CVE-2015-5317	Jenkins User Interface (UI) Information Disclosure Vulnerability	Jenkins Kernel	5.0	✗	✓	June 2, 2023
CVE-2016-3427	Oracle Java SE and JRockit Unspecified Vulnerability	Oracle Jenkins User Interface (UI)	9.0	✗	✓	June 2, 2023

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2016-8735	Apache Tomcat Remote Code Execution Vulnerability	Apache Java SE and JRockit	9.8	✗	✓	June 2, 2023
CVE-2004-1464	Cisco IOS Denial-of-Service Vulnerability	Cisco Tomcat	5.0	✗	✓	June 9, 2023
CVE-2016-6415	Cisco IOS, IOS XR, and IOS XE IKEv1 Information Disclosure Vulnerability	Cisco IOS	7.5	✓	✓	June 9, 2023
CVE-2023-21492	Samsung Mobile Devices Insertion of Sensitive Information Into Log File Vulnerability	Samsung IOS, IOS XR, and IOS XE	4.4	✓	✓	June 9, 2023
CVE-2023-32409	Apple Multiple Products WebKit Sandbox Escape Vulnerability	Apple Webkit Mobile Devices	-	✓	✓	June 12, 2023
CVE-2023-28204	Apple Multiple Products WebKit Out-of-Bounds Read Vulnerability	Apple Webkit Multiple Products	-	✓	✓	June 12, 2023
CVE-2023-32373	Apple Multiple Products WebKit Use-After-Free Vulnerability	Apple Webkit Multiple Products	-	✓	✓	June 12, 2023
CVE-2023-2868	Barracuda Networks ESG Appliance Improper Input Validation Vulnerability	Barracuda Networks Email Security Gateway (ESG) Appliance	9.4	✓	✓	June 16, 2023
CVE-2023-28771	Zyxel Multiple Firewalls OS Command Injection Vulnerability	Zyxel Multiple Firewalls	9.8	✗	✓	June 21, 2023

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-1389	✗	Archer AX21: before 1.1.4 20230219	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:tp-link:archer_ax21:*:*:*:*:*:*:*:*	Mirai Botnet
TP-Link Archer AX-21 Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1189: Drive-By Compromise	https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-45046	Log4j	All versions from 2.0-beta9 to 2.15.0, excluding 2.12.2	MuddyWater, Lazarus Group, Mint Sandstorm
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:log4j:2.0:-:*:*:*:*:*:*	Mirai botnet, Kinsing cryptomining, Tsunami botnet, Prophet Spider, EnemyBot, Conti Ransomware
Apache Log4j2 Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1203: Exploitation for Client Execution	https://logging.apache.org/log4j/2.x/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-21839	✗	Oracle WebLogic Server v 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:weblogic_server:12.2.1.3.0:*:*:*:*:*:*:*	-
Oracle WebLogic Server Unspecified Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1133:External Remote Services	https://www.oracle.com/security-alerts/cpujan2023.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29336	✗	Windows: 10 - 10 S Windows Server: 2008 - 2016	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_10_1507:*:*:*:*:*:*:*:*	-
Microsoft Win32K Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29336

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-25717	✗	RUCKUS H, T, E series, SmartZone, ZoneDirector	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ruckuswireless:ruckus_wireless_admin:*:*:*:*:*:*:*:*	Andoryu botnet
Multiple Ruckus Wireless Products CSRF and RCE Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1133:External Remote Services	https://support.ruckuswireless.com/security_bulletins/315

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-3560	✗	redhat-virtualization-host (Red Hat package): 4.4.6-20210527.3.el8_4 - 4.4.6-20210527.3.el8_4, redhat-release-virtualization-host (Red Hat package): 4.4.6-1.el8ev - 4.4.6-1.el8ev, Red Hat Virtualization Host: 4 – 4, Red Hat Virtualization: 4 - 4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:polkit_project:polkit:*:*:*:*:*:*:*:*	-
Red Hat Polkit Incorrect Authorization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-754 CWE-863	T1068: Exploitation for Privilege Escalation	https://bugzilla.redhat.com/show_bug.cgi?id=1961710

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-0196	✗	SUSE Linux: 11 - 11	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Race Condition Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-362	T1068: Exploitation for Privilege Escalation	https://lkml.iu.edu/hypermail/linux/kernel/1609.1/02103.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2010-3904	✗	Linux kernel before 2.6.36	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Improper Input Validation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1068: Exploitation for Privilege Escalation	https://lkml.iu.edu/hypermail/linux/kernel/1601.3/06474.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-5317	✗	Jenkins User Interface (UI)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:jenkins:jenkins:*:*:*:*:*:*:*:*; cpe:2.3:a:jenkins:jenkins:*:*:*:*:lts:*:*:*	-
Jenkins User Interface (UI) Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-28252

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-3427	✗	Java SE: 6u113, 7u99, 8u77; Java SE Embedded: 8u77; JRockit: R28.3.9	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:jrockit:*:*:*:*:*:*:*:*	-
Oracle Java SE and JRockit Unspecified Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-829	T1190: Exploit Public-Facing Application, T1191: Exploit Web Service	https://www.oracle.com/security-alerts/cpuapr2016v3.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-8735	⊗	Apache Tomcat: 6.0.0 - 9.0.0-M11	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:tomcat:-:*:*:*:*:*:	-
Apache Tomcat Remote Code Execution Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1203: Exploitation for Client Execution	https://tomcat.apache.org/security-9.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2004-1464	⊗	Cisco IOS 9.x, 10.x, 11.x and 12.x	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:ios:*:*:*:*:*:*:*:*	-
Cisco IOS Denial-of-Service Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-400	T1498: Network Denial of Service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-6415	✗	Cisco IOS: 12.0 - 15.2.4 ea Cisco IOS XR: 5.1.0 - 6.0.1 Cisco IOS XE: 3.15S - 3.17S	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:ios:*:*:*:*:*:*:*:*	-
Cisco IOS, IOS XR, and IOS XE IKEv1 Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1082: System Information Discovery	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-21492	✗	Samsung Mobile Firmware: before SMR-MAY-2023	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:samsung:android:11.0:-:*:*:*:*:*:*	-
Samsung Mobile Devices Insertion of Sensitive Information Into Log File Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-532	T1190: Exploit Public-Facing Application	https://security.samsungmobile.com/securityUpdate.smsb

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32409	✗	WebKitGTK+: All versions WPE WebKit: All versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:webkitgtk:webkitgtk:*:*:*:*:*:*:*:*	-
Apple Multiple Products WebKit Sandbox Escape Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1203: Exploitation for Client Execution; T1497: Virtualization/Sandbox Evasion	https://support.apple.com/HT213757, https://support.apple.com/HT213758, https://support.apple.com/HT213761, https://support.apple.com/HT213762, https://support.apple.com/HT213764, https://support.apple.com/HT213765

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28204	✗	WebKitGTK+: 2.40.0 - 2.40.1 WPE WebKit: 2.40.0 - 2.40.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:webkitgtk:webkitgtk:2.40.1:*:*:*:*:*:*:*	-
Apple Multiple Products WebKit Out-of-Bounds Read Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1203: Exploitation for Client Execution	https://support.apple.com/HT213757, https://support.apple.com/HT213758, https://support.apple.com/HT213761, https://support.apple.com/HT213762, https://support.apple.com/HT213764, https://support.apple.com/HT213765

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32373	✗	WebKitGTK+: 2.40.0 - 2.40.1 WPE WebKit: 2.40.0 - 2.40.1	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:webkitgtk:webkitgtk:2.40.1:*:*:*:*:*:*:*	-
Apple Multiple Products WebKit Use-After-Free Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-416	T1203: Exploitation for Client Execution	https://support.apple.com/HT213757, https://support.apple.com/HT213758, https://support.apple.com/HT213761, https://support.apple.com/HT213762, https://support.apple.com/HT213764, https://support.apple.com/HT213765

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-2868	✗	Barracuda Networks Email Security Gateway (ESG): 5.1.3 - 9.2	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:barracuda_networks:esg:9.2:*:*:*:*:*:*:*	-
Barracuda Networks ESG Appliance Improper Input Validation Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-20	T1059: Command and Scripting Interpreter	https://status.barracuda.com/incidents/34kx82j5n4q9

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28771	✗	ATP series: 4.60 - 5.35; USG FLEX series: 4.60 - 5.35; VPN series: 4.60 - 5.35; ZyWALL: 4.60 - 4.73 USG series: 4.60 - 4.73	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:o:zyxel:atp100_firmware:*:*:*:*:*:*:*:*	-
Zyxel Multiple Firewalls OS Command Injection Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-78	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls

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.

Contextualize
Uni5 Threat Exposure Management
Prioritize
Resolve

REPORT GENERATED ON

June 1, 2023 • 3:40 AM

More at www.hivepro.com