

Date of Publication
July 3, 2023



HiveForce Labs

CISA

KNOWN

EXPLOITED

VULNERABILITY

CATALOG

June 2023

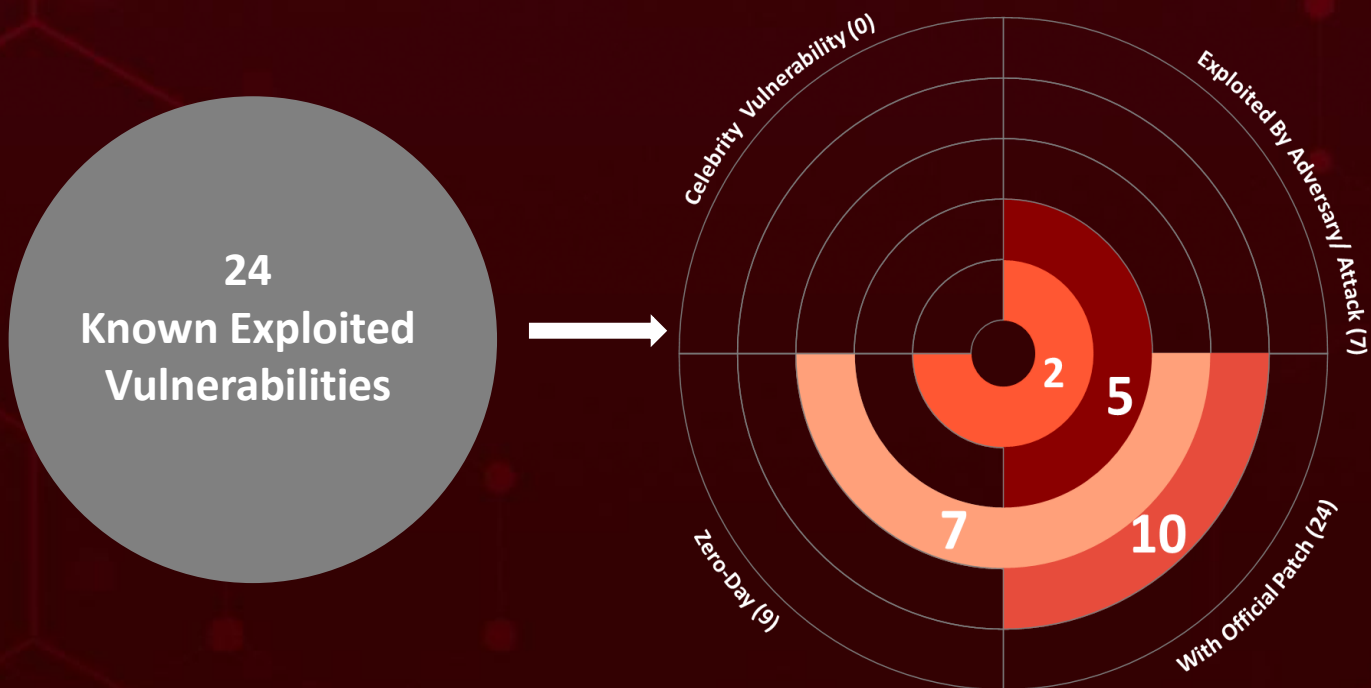
Table of Contents

<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	06
<u>Recommendations</u>	18
<u>References</u>	19
<u>Appendix</u>	19
<u>What Next?</u>	20

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 June 2023, 24 vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, nine are zero-day vulnerabilities; seven 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-2023-3079	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8 Engine	8.8			June 28, 2023
CVE-2023-33009	Zyxel Multiple Firewalls Buffer Overflow Vulnerability	Zyxel Multiple Firewalls	9.8			June 26, 2023
CVE-2023-33010	Zyxel Multiple Firewalls Buffer Overflow Vulnerability	Zyxel Multiple Firewalls	9.8			June 26, 2023
CVE-2023-34362	Progress MOVEit Transfer SQL Injection Vulnerability	Progress MOVEit Transfer	9.8			June 23, 2023
CVE-2023-32439	Apple Multiple Products WebKit Type Confusion Vulnerability	Apple Multiple Products	8.8			July 14, 2023
CVE-2023-20867	VMware Tools Authentication Bypass Vulnerability	VMware Tools	3.9			July 14, 2023
CVE-2023-27992	Zyxel Multiple NAS Devices Command Injection Vulnerability	Zyxel Multiple Network-Attached Storage (NAS) Devices	9.8			July 14, 2023
CVE-2023-20887	Vmware Aria Operations for Networks Command Injection Vulnerability	VMware Aria Operations for Networks	9.8			July 13, 2023
CVE-2020-35730	Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability	Roundcube Webmail	6.1			July 13, 2023
CVE-2020-12641	Roundcube Webmail Remote Code Execution Vulnerability	Roundcube Webmail	9.8			July 13, 2023
CVE-2021-44026	Roundcube Webmail SQL Injection Vulnerability	Roundcube Webmail	9.8			July 13, 2023
CVE-2016-9079	Mozilla Firefox, Firefox ESR, and Thunderbird Use-After-Free Vulnerability	Mozilla Firefox, Firefox ESR, & Thunderbird	7.5			July 13, 2023




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2016-0165	Microsoft Win32k Privilege Escalation Vulnerability	Microsoft Win32k	7.8			July 13, 2023
CVE-2023-27997	Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS and FortiProxy SSL-VPN	9.8			July 4, 2023
CVE-2019-17621	D-Link DIR-859 Router Command Execution Vulnerability	D-Link DIR-859 Router	9.8			July 20, 2023
CVE-2019-20500	D-Link DWL-2600AP Access Point Command Injection Vulnerability	D-Link DWL-2600AP Access Point	7.8			July 20, 2023
CVE-2021-25487	Samsung Mobile Devices Out-of-Bounds Read Vulnerability	Samsung Mobile Devices	7.8			July 20, 2023
CVE-2021-25489	Samsung Mobile Devices Improper Input Validation Vulnerability	Samsung Mobile Devices	5.5			July 20, 2023
CVE-2021-25394	Samsung Mobile Devices Race Condition Vulnerability	Samsung Mobile Devices	6.4			July 20, 2023
CVE-2021-25395	Samsung Mobile Devices Race Condition Vulnerability	Samsung Mobile Devices	6.4			July 20, 2023
CVE-2021-25371	Samsung Mobile Devices Unspecified Vulnerability	Samsung Mobile Devices	6.7			July 20, 2023
CVE-2021-25372	Samsung Mobile Devices Improper Boundary Check Vulnerability	Samsung Mobile Devices	6.7			July 20, 2023
CVE-2023-32434	Apple Multiple Products Integer Overflow Vulnerability	Apple Multiple Products	7.8			July 14, 2023
CVE-2023-32435	Apple Multiple Products WebKit Memory Corruption Vulnerability	Apple Multiple Products	8.8			July 14, 2023







CVEs Details




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3079		Google Chrome: 100.0.4896.60 - 114.0.5735.91	-
	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	https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop.html
	CWE-843		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34362		MOVEit Transfer: 2021.0 - 2023.0	Lace Tempest(aka FIN11) & TA505 (aka GracefulSpider)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:progress:moveit_cloud:*:*:*:*:*:*	Clop Ransomware
Progress MOVEit Transfer SQL Injection Vulnerability			
	CWE ID	T1059: Command and Scripting Interpreter	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
	CWE-89		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33009		ATP series: 4.32-5.36,USG FLEX series: 4.50-5.36,USG FLEX 50W: 4.25-5.36,USG20W-VPN: 4.25-5.36,VPN series: 4.30-5.36,ZyWALL: 4.25-4.73,USG series: 4.25-4.73	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:zyxel:atp100_firmware:*:*:*:*:*:*	-
Zyxel Multiple Firewalls Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	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	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20867		VMware tools: 10.1.15 - 12.2.0	UNC3886
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:tools:*:*:*:*:*	VirtualPita and VirtualPie backdoors
VMware Tools Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application,T1040: Network Sniffing	https://www.vmware.com/security/advisories/VMSA-2023-0013.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33010		ATP series:4.32-5.36,USG FLEX series:4.50-5.36,USG FLEX 50W:4.25-5.36,USG20W-VPN:4.25-5.36,VPN series:4.30-5.36,ZyWALL:4.25-4.73,USG series:4.25-4.73	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:zyxel:atp100_firmware:*.:*:*:*:*:*:*	-
Zyxel Multiple Firewalls Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	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	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32439		WPE WebKit: before 2.40.0, WebKitGTK+: before 2.40.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:webkitgtk:wpe_webkit:*.:*:*:*:*:*:*	-
Apple Multiple Products WebKit Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/HT213816




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27992		NAS326 Version-5.21(AAZF.13)C0 and earlier,NAS540 Version-5.21(AATB.10)C0 and earlier,NAS542 Version-5.21(ABAG.10)C0 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:zyxel:nas326_firmware:*:*:*:*:*:*:*:*	-
Zyxel Multiple NAS Devices 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-pre-authentication-command-injection-vulnerability-in-nas-products




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20887		VMware Aria Operations for Networks: 6.0.0 - 6.8.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:vr_realize_network_insight:*:*:*:*:*:*:*	-
Vmware Aria Operations for Networks Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://www.vmware.com/security/advisories/VMSA-2023-0012.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2020-35730</u>		Roundcube: 1.2.0 - 1.4.9	APT28 (aka Fancy Bear)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*	-
Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1059.007: JavaScript/JScript, T1557: Man-in-the-Browser, T1189: Drive-by Compromise, T1204: User Execution, T1204.001: Malicious Link	https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2020-12641</u>		Roundcube: 1.2.0 - 1.4.3	APT28 (aka Fancy Bear)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*	-
Roundcube Webmail Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://roundcube.net/news/2020/04/29/security-updates-1.4.4-1.3.11-and-1.2.10




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44026		Roundcube: 1.3.0 - 1.4.11	APT28 (aka Fancy Bear)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS		
Roundcube Webmail SQL Injection Vulnerability		cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1505: Server Software Component, T1505.003: Web Shell, T1136: Create Account, T1190: Exploit Public-Facing Application, T1565.001: Data Manipulation	https://roundcube.net/news/2021/11/12/security-updates-1.4.12-and-1.3.17-released

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-9079		Mozilla Firefox: 49.0 - 50.0.2 & Mozilla Thunderbird: 45.0 - 45.5.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*	
Mozilla Firefox, Firefox ESR, and Thunderbird Use-After-Free Vulnerability		cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter	https://www.mozilla.org/en-US/security/advisories/mfsa2016-92/#CVE-2016-9079

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-0165		Windows: 7 – Vista & Windows Server: 2008 - 2012 R2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows_vista.*:sp2.*:*:*:*:*:*	-
Microsoft Win32k Privilege Escalation Vulnerability		cpe:2.3:o:microsoft:windows_server.*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264	T1068: Exploitation for Privilege Escalation, T1204: User Execution, T1204.001:Malicious Link	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-039




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27997		FortiOS: 6.0.0 - 7.2.4, FortiProxy: 1.1.0 - 7.2.3 & FortiOS-6K7K: 6.0.10 - 7.0.10	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:fortinet:fortios.*:*:*:*:*:*	-
Fortinet FortiOS and FortiProxy SSL-VPN Heap-Based Buffer Overflow Vulnerability		cpe:2.3:a:fortinet:fortiproxy.*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	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	https://www.fortiguard.com/psirt/FG-IR-23-097




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-17621		DIR-859: 1.05 - 1.06b01Beta01	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:dlink:dir-859:-:*:*:*:*:*:*	Mirai botnet
D-Link DIR-859 Router Command Execution Vulnerability			
	CWE ID		
	CWE-78	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10147




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-20500		DWL-2600AP Revision A : 4.2.0.15 and older	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:dlink:dwl-2600ap:-:*:*:*:*:*:*	Mirai botnet
D-Link DWL-2600AP Access Point Command Injection Vulnerability			
	CWE ID		
	CWE-78	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10113




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-25487		Exynos devices versions: O(8.1), P(9.0), Q(10.0), R(11.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:samsung:exynos:- :*:*:*:*:*:*	-
Samsung Mobile Devices Out-of-Bounds Read Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1005: Data from Local System, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1211: Exploitation for Defense Evasion, T1212: Exploitation for Credential Access	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-25489		Exynos devices versions: O(8.1), P(9.0), Q(10.0), R(11.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:samsung:exynos:- :*:*:*:*:*:*	-
Samsung Mobile Devices Improper Input Validation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-134 CWE-20	T1068: Exploitation for Privilege Escalation	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-25394		Exynos and Qualcomm devices versions: O(8.1), P(9.0), Q(10.0), R(11.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:samsung:exynos:- .*.*.*.*.*.*.*.*	-
Samsung Mobile Devices Race Condition Vulnerability		cpe:2.3:o:google:android:.*.*.*.*.*.*.*.*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416 CWE-362	T1068: Exploitation for Privilege Escalation	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=5

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-25395		Exynos and Qualcomm devices versions: O(8.1), P(9.0), Q(10.0), R(11.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:samsung:exynos:- .*.*.*.*.*.*.*.*	-
Samsung Mobile Devices Race Condition Vulnerability		cpe:2.3:o:google:android:.*.*.*.*.*.*.*.*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-362	T1068: Exploitation for Privilege Escalation	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=5

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-25371		Samsung Mobile Firmware: before SMR-MAR-2021	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:samsung:samsung_mobile_firmware:*.:.:.:.:.*:	-
Samsung Mobile Devices Unspecified Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-912	T1190: Exploit Public-Facing Application, T1191: Exploit Web Service	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=3

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-25372		Samsung Mobile Firmware: before SMR-MAR-2021	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:samsung:samsung_mobile_firmware:*.:.:.:.:.*:	-
Samsung Mobile Devices Improper Boundary Check Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1068: Exploitation for Privilege Escalation	https://security.samsungmobile.com/securityUpdate.smsb?year=2021&month=3

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32434		Apple iOS: 15.0 19A346 - 15.7.6 19H349, iPadOS: 15.0 19A346 - 15.7.6 19H349	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*	-
Apple Multiple Products 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	https://support.apple.com/en-us/HT213814

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32435		Apple iOS: 15.0 19A346 - 15.7.6 19H349, iPadOS: 15.0 19A346 - 15.7.6 19H349	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*	-
Apple Multiple Products WebKit Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1005: Data from Local System, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1211: Exploitation for Defense Evasion, T1212: Exploitation for Credential Access	https://support.apple.com/en-us/HT213676

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 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

July 3, 2023 • 10:16 PM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com