Date of Publication
October 2, 2023

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

September 2023

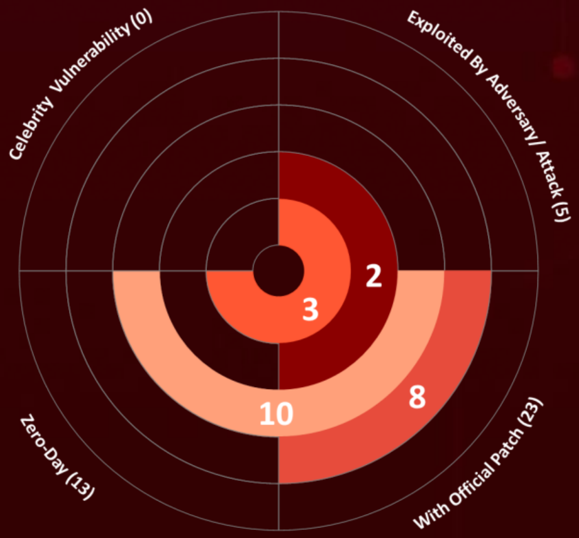
Table of Contents

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

23
Known Exploited
Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-41991	Apple Multiple Products Improper Certificate Validation Vulnerability	Apple Multiple Products	5.5	✓	✓	Oct 16, 2023
CVE-2023-41992	Apple Multiple Products Kernel Privilege Escalation Vulnerability	Apple Multiple Products	7.8	✓	✓	Oct 16, 2023
CVE-2023-41993	Apple Multiple Products WebKit Code Execution Vulnerability	Apple Multiple Products	9.8	✓	✓	Oct 16, 2023
CVE-2023-41179	Trend Micro Apex One and Worry-Free Business Security Remote Code Execution Vulnerability	Trend Micro Apex One and Worry-Free Business Security	7.2	✓	✓	Oct 12, 2023
CVE-2023-28434	MinIO Security Feature Bypass Vulnerability	MinIO MinIO	8.8	✓	✓	Oct 10, 2023
CVE-2022-22265	Samsung Mobile Devices Use-After-Free Vulnerability	Samsung Mobile Devices	7.8	✗	✓	Oct 9, 2023
CVE-2014-8361	Realtek SDK Improper Input Validation Vulnerability	Realtek SDK	-	✗	✓	Oct 9, 2023
CVE-2017-6884	Zyxel EMG2926 Routers Command Injection Vulnerability	Zyxel EMG2926 Routers	8.8	✗	✓	Oct 9, 2023
CVE-2021-3129	Laravel Ignition File Upload Vulnerability	Laravel Ignition	9.8	✗	✓	Oct 9, 2023
CVE-2022-31459	Owl Labs Meeting Owl Inadequate Encryption Strength Vulnerability	Owl Labs Meeting Owl	6.5	✗	✓	Oct 16, 2023

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2022-31461	Owl Labs Meeting Owl Missing Authentication for Critical Function Vulnerability	Owl Labs Meeting Owl	6.5	✗	✓	Oct 16, 2023
CVE-2022-31462	Owl Labs Meeting Owl Use of Hard-coded Credentials Vulnerability	Owl Labs Meeting Owl	8.8	✗	✓	Oct 16, 2023
CVE-2022-31463	Owl Labs Meeting Owl Improper Authentication Vulnerability	Owl Labs Meeting Owl	7.1	✗	✓	Oct 16, 2023
CVE-2023-26369	Adobe Acrobat and Reader Out-of-Bounds Write Vulnerability	Adobe Acrobat and Reader	7.8	✓	✓	Oct 5, 2023
CVE-2023-35674	Android Framework Privilege Escalation Vulnerability	Android Framework	7.8	✓	✓	Oct 4, 2023
CVE-2023-20269	Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability	Cisco Adaptive Security Appliance and Firepower Threat Defense	9.1	✓	✓	Oct 4, 2023
CVE-2023-4863	Google Chromium WebP Heap-Based Buffer Overflow Vulnerability	Google Chromium WebP	8.8	✓	✓	Oct 4, 2023
CVE-2023-36761	Microsoft Word Information Disclosure Vulnerability	Microsoft Word	5.3	✓	✓	Oct 3, 2023
CVE-2023-36802	Microsoft Streaming Service Proxy Privilege Escalation Vulnerability	Microsoft Streaming Service Proxy	7.8	✓	✓	Oct 3, 2023
CVE-2023-41064	Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow Vulnerability	Apple iOS, iPadOS, and macOS	7.8	✓	✓	Oct 2, 2023

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-41061	Apple iOS, iPadOS, and watchOS Wallet Code Execution Vulnerability	Apple iOS, iPadOS, and watchOS	7.8	✓	✓	Oct 10, 2023
CVE-2023-33246	Apache RocketMQ Command Execution Vulnerability	Apache RocketMQ	9.8	✗	✓	Sep 27, 2023
CVE-2018-14667	Red Hat JBoss RichFaces Framework Expression Language Injection Vulnerability	Red Hat JBoss RichFaces Framework	9.8	✗	✓	Oct 19, 2023

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41991	✗	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	-
	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:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	Predator
Apple Multiple Products Improper Certificate Validation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-295	T1587.003: Develop Capabilities: Digital Certificates	https://support.apple.com/en-us/HT213927; https://support.apple.com/en-us/HT213931

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41992	✗	iPhone, iOS, iPadOS, macOS, watchOS, and Safari	-
	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:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	Predator
Apple Multiple Products Kernel Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK

	CWE-754	T1068: Exploitation for Privilege Escalation	https://support.apple.com/en-us/HT213927;
			https://support.apple.com/en-us/HT213931;
			https://support.apple.com/en-us/HT213932

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2023-41993](https://nvd.nist.gov/vuln/detail/CVE-2023-41993)	✗	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	-
	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:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	Predator
Apple Multiple Products WebKit Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS

	CWE-754	T1068: Exploitation for Privilege Escalation	https://support.apple.com/en-us/HT213927;
			https://support.apple.com/en-us/HT213931;
			https://support.apple.com/en-us/HT213932

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41179	✗	Apex One: 2019 - SP1 b11564 Worry-Free Business Security: 9.5 - xg	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:trendmicro:apex_one:2019:*:*:*:*:*:*:*	-
Trend Micro Apex One and Worry-Free Business Security Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-78	T1203: Exploitation for Client Execution	https://success.trendmicro.com/solution/000294994

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28434	✗	minio: 2019-12-17T23-16-33Z - 2023-03-13T19-46-17Z	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:minio:minio:*:*:*:*:*:*:*:*	-
MinIO Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-269	T1068: Exploitation for Privilege Escalation	https://github.com/minio/minio/commit/67f4ba154a27a1b06e48bfabda38355a010dfca5

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-22265	✗	Samsung Mobile Devices	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:samsung:exynos:-:*:*:*:*:*:*:*	-
Samsung Mobile Devices Use-After-Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-703	T1068- Exploitation for Privilege- Escalation, T1190- Exploit Public-Facing- Application, T1203: Exploitation for Client Execution	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-8361	✗	Realtek SDK: All versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:realtek:realtek_sdk:-:*:*:*:*:*:*:*	HinataBot, Gafgyt botnet
Realtek SDK Improper Input Validation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1068- Exploitation for Privilege- Escalation, T1203: Exploitation for Client Execution	http://securityadvisories.dlink.com/security/publication.aspx?name=SAP10055

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-6884	✗	Zyxel EMG2926-Q10A: 1.00(AAQT.4)b8	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:zyxel:emg2926_firmware:v1.00\(aaqt.4\)b8:*:*:*:*:*:*:* cpe:2.3:h:zyxel:emg2926:-:*:*:*:*:*:*:*	-
Zyxel EMG2926 Routers Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-78	T1055: Process Injection, T1059: Command and Scripting Interpreter	https://www.exploitdb.com/exploits/41782/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-3129	✗	Ignition: 1.16.0 - 1.16.4	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:facade:ignition:*:*:*:*:*:laravel:*:*	-
Laravel Ignition File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-94	T1105: Ingress Tool Transfer	https://github.com/facade/ignition/releases/tag/2.5.2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-31459	⊗	Owl Labs Meeting Owl version 5.4.1.3 or before versions	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:owllabs:meeting_owl_pro_firmware:*:*:*:*:*:*:*:*	-
Owl Labs Meeting Owl Inadequate Encryption Strength Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-306	T1027: Obfuscated Files or Information	https://resources.owllabs.com/blog/owl-labs-update

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-31461	⊗	Owl Labs Meeting Owl version 5.4.1.3 or before versions	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:owllabs:meeting_owl_pro_firmware:*:*:*:*:*:*:*:*	-
Owl Labs Meeting Owl Missing Authentication for Critical Function Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-306	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://resources.owllabs.com/blog/owl-labs-update

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-31462	❌	Owl Labs Meeting Owl version 5.4.1.3 or before versions	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:owllabs:meeting_owl_pro_firmware:*:*:*:*:*:*:*:*	-
Owl Labs Meeting Owl Use of Hard-coded Credentials Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-798	T0891: Hardcoded Credentials	https://resources.owllabs.com/blog/owl-labs-update

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-31463	❌	Owl Labs Meeting Owl version 5.4.1.3 or before versions	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:owllabs:meeting_owl_pro_firmware:*:*:*:*:*:*:*:*	-
Owl Labs Meeting Owl Improper Authentication Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://resources.owllabs.com/blog/owl-labs-update

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26369	✗	Acrobat DC 23.003.20284 and earlier versions, Acrobat Reader DC 23.003.20284 and earlier versions, Acrobat 2020 20.005.30516 (Mac) 20.005.30514 (Win) and earlier versions, Acrobat Reader 2020 20.005.30516 (Mac) 20.005.30514 (Win) and earlier versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:acrobat:*:*:*:*:classic:*:*:*	-
Adobe Acrobat and Reader Out-of-Bounds Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-787	T1599: Network Boundary Bridging	https://helpx.adobe.com/security/products/acrobat/apsb23-34.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35674	✗	Google Android: before 13 2023-09-01	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:*:*:*:*:*:*:*:*	-
Android Framework Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS

	CWE-20	T1203: Exploitation for Client Execution;
		T1059: Command and Scripting Interpreter;
		T1068:Exploitation for Privilege Escalation
			https://source.android.com/security/bulletin/2023-09-01

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2023-20269]()	✗	Cisco Adaptive Security Appliance (ASA) 6.2.3 - 9.19.1.18 and Cisco Firepower Threat Defense (FTD) 6.2.3 - 9.19.1.18	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:adaptive_security_appliance_software:6.2.3:*:*:*:*:*:*:*	-
Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-863	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://source.android.com/security/bulletin/2023-09-01

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4863	✗	Google Chrome version 116.0.5845.186 and before	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium WebP Heap-Based Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-787	T1190: Exploit Public-Facing Application, T1189: Drive-by Compromise	https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36761	✗	Microsoft Office: 365 - 2019 Microsoft Word: before 16.0.5413.1000 Microsoft 365 Apps for Enterprise: before 16.0.5413.1000	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:365_apps:-:*:*:*:enterprise:*:x64:* cpe:2.3:a:microsoft:office:2019:*:*:*:*:*:x64:* cpe:2.3:a:microsoft:word:2013:sp1:*:*:*:*:x64:*	-
Microsoft Word Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-668	T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36761

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36802	✗	Windows: 10 - 11 22H2 Windows Server: 2019 - 2022 20H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Microsoft Streaming Service Proxy Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-119	T1090: Proxy, T1068:Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36802

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41064	✗	iPhone 8 and later, iPad Pro (all models), iPad Air 3rd generation and later, iPad 5th generation and Later, iPad mini 5th generation and later, Macs running macOS Ventura	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-120	T1190: Exploit Public-Facing Application, T1189: Drive-by Compromise	https://support.apple.com/en-us/HT213905, https://support.apple.com/en-us/HT213906

CVE ID	**CELEBRITY VULNERABILITY**	**AFFECTED PRODUCTS**	**ASSOCIATED ACTOR**
CVE-2023-41061	✗	iPhone 8 and later, iPad Pro (all models), iPad Air 3rd generation and later, iPad 5th generation and Later, iPad mini 5th generation and later, Macs running macOS Ventura	-
	ZERO-DAY		
	✓		**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple iOS, iPadOS, and watchOS Wallet Code Execution Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**Mitigation DETAILS**
	CWE-20	T1203: Exploitation for Client Exécution, T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/HT213905, https://support.apple.com/kb/HT213907

CVE ID	**CELEBRITY VULNERABILITY**	**AFFECTED PRODUCTS**	**ASSOCIATED ACTOR**
CVE-2023-33246	✗	Apache RocketMQ: 4.2.0 - 5.1.0	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:apache:rocketmq:*:*:*:*:*:*:*:*	DreamBus Botnet
Apache RocketMQ Command Execution Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**Mitigation DETAILS**
	CWE-94	T1202: Indirect Command Execution, T1059: Command and Scripting Interpreter	https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-14667	⊗	JBoss Richfaces: 3.1.0 - 3.3.4	-
	ZERO-DAY		
	⊗		ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:redhat:richfaces:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:5.0:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*	-
Red Hat JBoss RichFaces Framework Expression Language Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-94	T1203: Exploitation for Client Exécution, T1059: Command and Scripting Interpreter, T1055: Process Injection	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-14667

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.

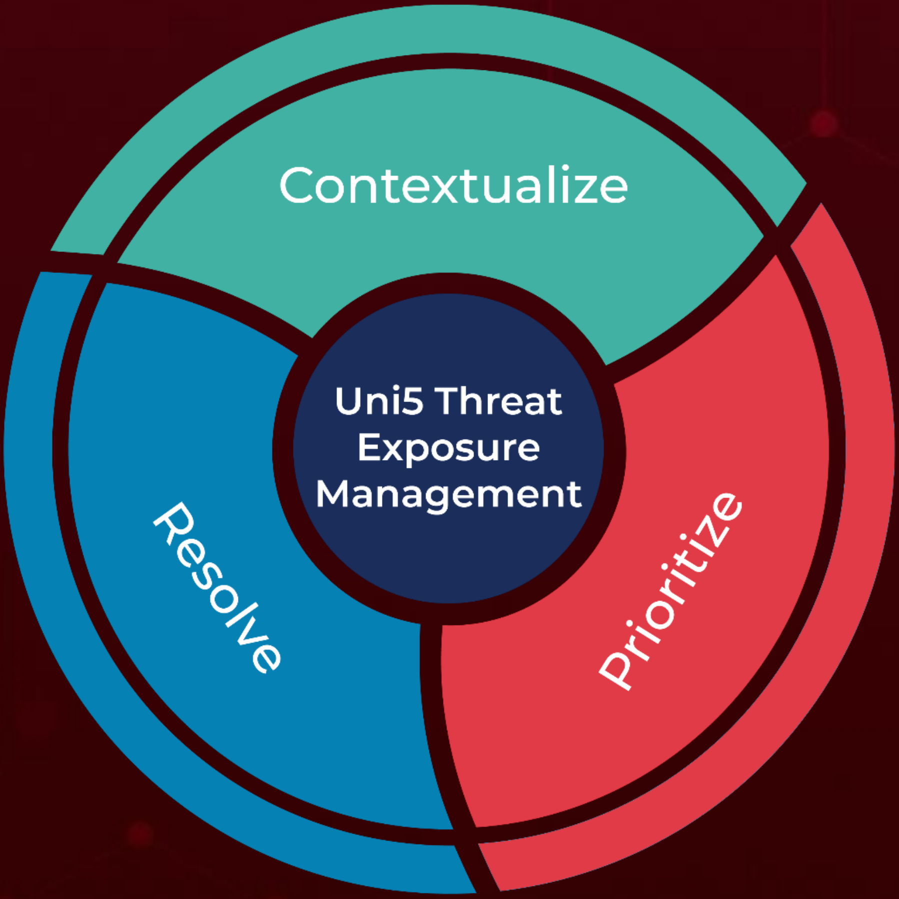
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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.



REPORT GENERATED ON

October 2, 2023 • 5:30 AM

More at www.hivepro.com