Date of Publication
January 9, 2024

Hive Pro®

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

December 2023

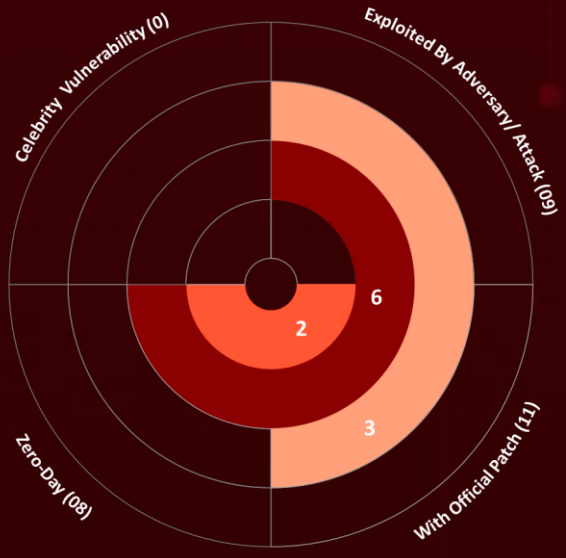
Table of Contents

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

11
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-42917	Apple Multiple Products WebKit Memory Corruption Vulnerability	Multiple Products	8.8	✓	✓	December 25, 2023
CVE-2023-42916	Apple Multiple Products WebKit Out-of-Bounds Read Vulnerability	Multiple Products	6.5	✓	✓	December 25, 2023
CVE-2023-33107	Qualcomm Multiple Chipsets Integer Overflow Vulnerability	Multiple Chipsets	7.8	✓	✓	December 26, 2023
CVE-2023-33106	Qualcomm Multiple Chipsets Use of Out-of-Range Pointer Offset Vulnerability	Multiple Chipsets	7.8	✓	✓	December 26, 2023
CVE-2023-33063	Qualcomm Multiple Chipsets Use-After-Free Vulnerability	Multiple Chipsets	7.8	✓	✓	December 26, 2023
CVE-2022-22071	Qualcomm Multiple Chipsets Use-After-Free Vulnerability	Multiple Chipsets	7.8	✗	✓	December 26, 2023
CVE-2023-41266	Qlik Sense Path Traversal Vulnerability	Sense	6.5	✗	✓	December 28, 2023
CVE-2023-41265	Qlik Sense HTTP Tunneling Vulnerability	Sense	9.9	✗	✓	December 28, 2023
CVE-2023-6448	Unitronics Vision PLC and HMI Insecure Default Password Vulnerability	Vision PLC and HMI	9.8	✓	✓	December 18, 2023
CVE-2023-49897	FXC AE1021, AE1021PE OS Command Injection Vulnerability	AE1021, AE1021PE	8.8	✓	✓	January 11, 2024
CVE-2023-47565	QNAP VioStor NVR OS Command Injection Vulnerability	VioStor NVR	8.8	✓	✓	January 11, 2024

CVEs Details

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-42917</td><td>  </td><td rowspan="2">iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, iPad mini 5th generation and later, Macs running macOS Monterey, Ventura, Sonoma</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Apple Multiple Products WebKit Memory Corruption Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-787</td><td>T1059: Command and Scripting Interpreter</td><td>https://support.apple.com/en-us/HT214031 , https://support.apple.com/en-us/HT214032 , https://support.apple.com/en-us/HT214033</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-42916</td><td>  </td><td rowspan="3">iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, iPad mini 5th generation and later, Macs running macOS Monterey, Ventura, Sonoma</td><td rowspan="3">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:*
cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Apple Multiple Products WebKit Out-of-Bounds Read Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-125</td><td>T1059: Command and Scripting Interpreter</td><td>https://support.apple.com/en-us/HT214031 , https://support.apple.com/en-us/HT214032 , https://support.apple.com/en-us/HT214033</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33107	✗ ZERO-DAY	Multiple Qualcomm Products	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qualcomm:315_5g_iot_modem_firmware:-:*:*:*:*:*:*:* cpe:2.3:h:qualcomm:315_5g_iot_modem:-:*:*:*:*:*:*:* cpe:2.3:o:qualcomm:apq8017_firmware:-:*:*:*:*:*:*:*	-
Qualcomm Multiple Chipsets Integer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1059: Command and Scripting Interpreter	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2024-bulletin.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33106	✗ ZERO-DAY	Multiple Qualcomm Products	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qualcomm:ar8035_firmware:-:*:*:*:*:*:*:* cpe:2.3:h:qualcomm:ar8035:-:*:*:*:*:*:*:*	-
Qualcomm Multiple Chipsets Use of Out-of-Range Pointer Offset Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1495: Firmware Corruption	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2024-bulletin.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33063		Multiple Qualcomm Products	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qualcomm:315_5g_iot_modem_firmware:-:*:*:*:*:*:*:* cpe:2.3:h:qualcomm:315_5g_iot_modem:-:*:*:*:*:*:*:* cpe:2.3:o:qualcomm:apq8017_firmware:-:*:*:*:*:*:*:*	-
Qualcomm Multiple Chipsets Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1021: Remote Services	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2024-bulletin.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-22071		Multiple Qualcomm Products	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qualcomm:apq8053_firmware:-:*:*:*:*:*:*:* cpe:2.3:h:qualcomm:apq8053:-:*:*:*:*:*:*:*	-
Qualcomm Multiple Chipsets Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1055.009: Proc Memory	https://docs.qualcomm.com/product/publicresources/securitybulletin/may-2022-bulletin.html

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-41266</td><td>  </td><td rowspan="2">Qlik Sense Enterprise for Windows: August 2022 Patch 12 - November 2022 Patch 10</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="3">cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:*
cpe:2.3:a:qlik:qlik_sense:august_2022:patch_1:*:*:enterprise:windows:*:*
pe:2.3:a:qlik:qlik_sense:february_2023:-:*:*:enterprise:windows:*:*
cpe:2.3:a:qlik:qlik_sense:february_2023:patch_1:*:*:enterprise:windows:*:*</td><td rowspan="3">Cactus ransomware</td></tr>
<tr><td rowspan="3">Qlik Sense Path Traversal Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-20</td><td>T1202: Indirect Command Execution,
T1059: Command and Scripting Interpreter</td><td>https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41265	✗	Qlik Sense Enterprise for Windows: August 2022 Patch 12 - November 2022 Patch 10	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:qlik:qlik_sense:august_2022:-:*:*:enterprise:windows:*:* cpe:2.3:a:qlik:qlik_sense:august_2022:patch_1:*:*:enterprise:windows:*:*	Cactus ransomware
Qlik Sense HTTP Tunneling Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-444	T1068: Exploitation for Privilege Escalation	https://community.qlik.com/t5/Product-Downloads/tkb-p/Downloads

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-6448	✗	Unitronics Vision: All versions	CyberAv3ngers
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:unitronics:vision1210_firmware:-:*:*:*:*:*:*:* cpe:2.3:h:unitronics:vision1210:-:*:*:*:*:*:*:*	-
Unitronics Vision PLC and HMI Insecure Default Password Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-798, CWE-1188	T1078.001: Default Accounts	https://www.unitronicsplc.com/software-visilogic-for-programmable-controllers/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-49897	✗	AE1021PE: 2.0.9 AE1021: 2.0.9	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:fxc:ae1021_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:fxc:ae1021:-:*:*:*:*:*:*:* cpe:2.3:o:fxc:ae1021pe_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:fxc:ae1021pe:-:*:*:*:*:*:*:*	InfectedSlurs, JenX Mirai
FXC AE1021, AE1021PE OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter T1055: Process Injection	https://jvn.jp/en/vu/JVNVU92152057/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-47565	✗	QVR: before 5.0.0	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qnap:qvr_firmware:*:*:*:*:*:*:*:*	InfectedSlurs, JenX Mirai
QNAP VioStor NVR OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter T1055: Process Injection	https://www.qnap.com/en/download

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.

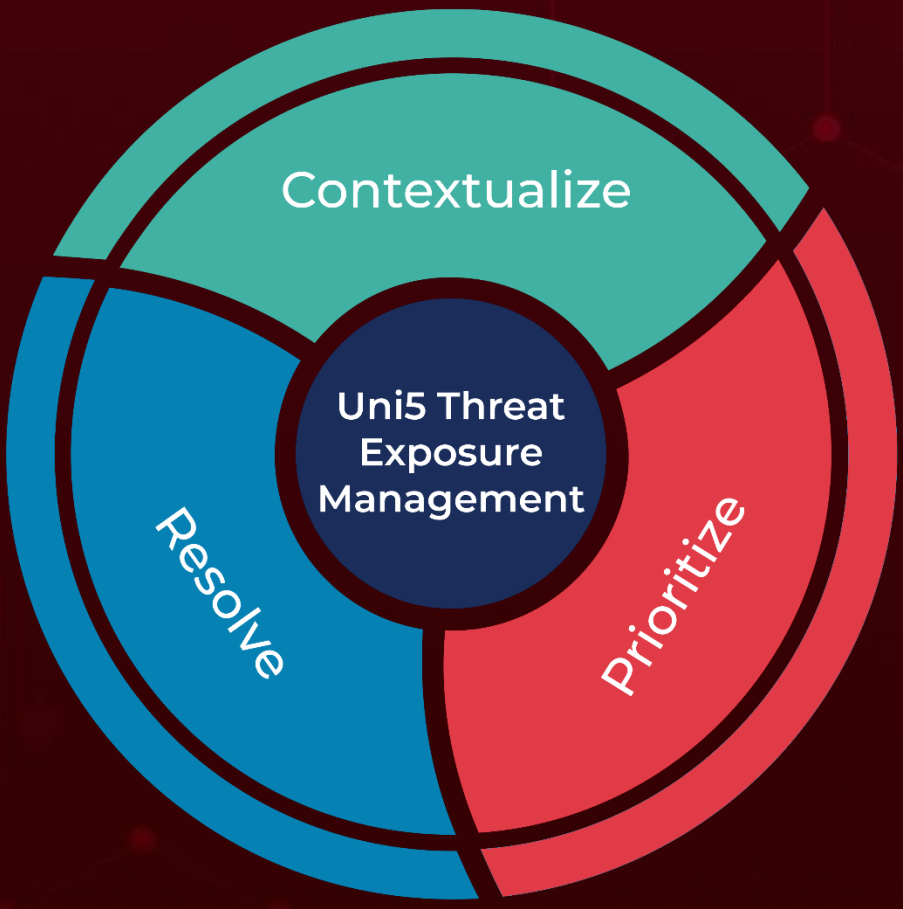
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

January 9, 2024 . 4:20 AM

More at www.hivepro.com