

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Apple Patches Three Exploited Zero-Day Vulnerabilities in macOS

Date of Publication

May 19, 2023

Admiralty Code

A1

TA Number

TA2023236










Summary

First Seen: May 1, 2023

Affected Platforms: MacOS Ventura

Impact: The exploitation of three zero-day vulnerabilities in Apple devices could lead to unauthorized access, data breaches, privacy invasion.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-32409	Apple Sandbox Escape Vulnerability	macOS Ventura			
CVE-2023-28204	Apple Out-of-bounds read Vulnerability	macOS Ventura			
CVE-2023-32373	Apple use-after-free Vulnerability	macOS Ventura			

Vulnerability Details

#1

Apple has released security advisories addressing three new zero-day vulnerabilities that were exploited to hack into iPhones, Macs, and iPads. The vulnerabilities were found in the WebKit browser engine and are tracked as CVE-2023-32409, CVE-2023-28204, and CVE-2023-32373. The first vulnerability allows remote attackers to escape sandboxes, while the other two enable attackers to access sensitive information and execute arbitrary code after tricking users into loading malicious web pages.

#2

Apple has patched the vulnerabilities in various operating systems and Safari, including macOS Ventura 13.4. Apple has not disclosed details about the attacks exploiting these vulnerabilities. It's worth noting that Apple has addressed a total of six zero-days since the beginning of 2023, with some of them being part of state-backed campaigns and in-the-wild exploit chains.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-32409	macOS Ventura before 13.4	cpe:2.3:o:apple:macOS.*.*.*.*	CWE-119
CVE-2023-28204			CWE-125
CVE-2023-32373			CWE-416

Recommendations



To ensure protection against these vulnerabilities, users should promptly update their devices to the latest available software versions, including macOS. Keeping software up to date is crucial for maintaining the security and integrity of Apple devices.



Improved Bounds Checks: Apple has enhanced bounds checks to prevent attackers from exploiting the vulnerabilities related to out-of-bounds read and achieving arbitrary code execution.



Input Validation: The software updates include improved input validation mechanisms to mitigate the risk of attackers gaining access to sensitive information.



Memory Management: Apple has implemented enhanced memory management techniques to address the use-after-free vulnerability and prevent arbitrary code execution on compromised devices.

Potential MITRE ATT&CK TTPs

<u>TA0005</u> Defense Evasion	<u>TA0007</u> Discovery	<u>TA0002</u> Execution	<u>TA0040</u> Impact
<u>TA0003</u> Persistence	<u>T1203</u> Exploitation for Client Execution	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1497</u> Virtualization/Sandbox Evasion
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	

Patch Details

<https://support.apple.com/en-us/HT213758>

<https://support.apple.com/en-gb/HT201222>

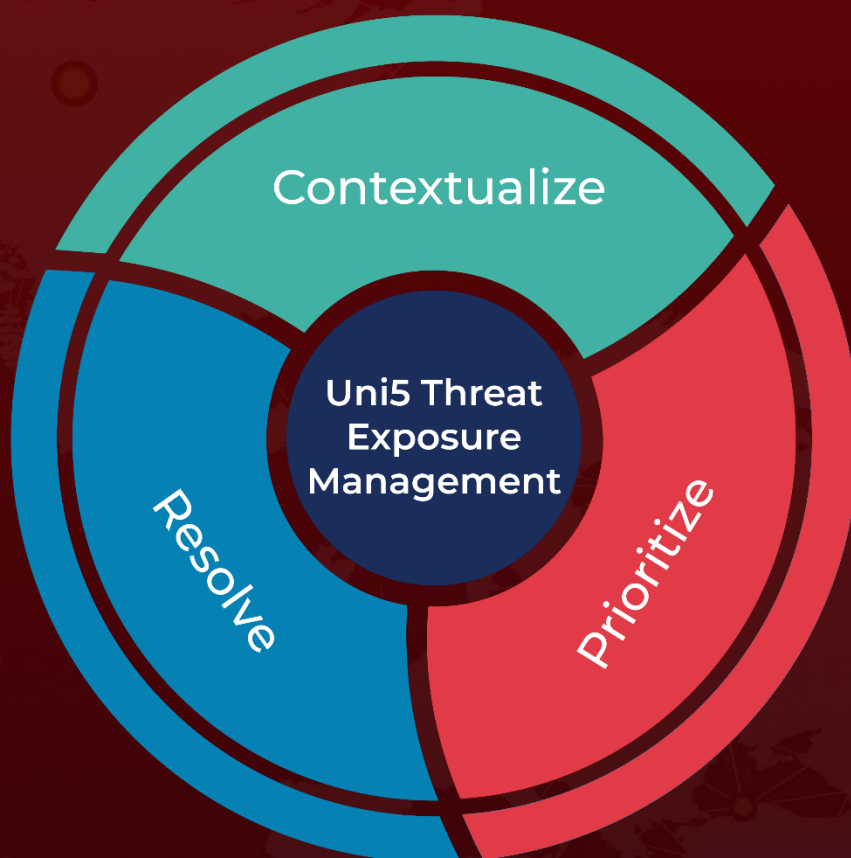
References

<https://www.bleepingcomputer.com/news/apple/apple-fixes-three-new-zero-days-exploited-to-hack-iphones-macs/>

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

May 19, 2023 • 4:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com