

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Apple's Timely Response to Actively Exploited Zero-Days

Date of Publication

December 13, 2023

Admiralty Code

A1

TA Number

TA2023501







Summary

First Seen: November 30, 2023

Affected Products: iPhone, iPad, and Macs running macOS Monterey, Ventura, Sonoma

Impact: Apple has released crucial software updates to address two actively exploited security vulnerabilities identified as CVE-2023-42916 and CVE-2023-42917. These vulnerabilities affect the WebKit browser engine on Apple devices such as iPhone, iPad, and Mac, potentially exposing sensitive information.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-42916	Apple WebKit Out-of-Bounds Read Vulnerability	Apple Multiple Products			
CVE-2023-42917	Apple WebKit Memory Corruption Vulnerability	Apple Multiple Products			

Vulnerability Details

#1

Apple has rolled out software updates to address two security vulnerabilities that have been actively exploited in the wild, particularly impacting older versions of its software. These vulnerabilities are identified as CVE-2023-42916 and CVE-2023-42917, and they specifically affect the WebKit browser engine on Apple devices, including the iPhone, iPad, and Mac.

#2

The first zero-day vulnerability, CVE-2023-42916, is related to an out-of-bounds read issue. Exploiting this flaw could potentially expose sensitive information by enticing users to interact with specially crafted web content. The second vulnerability, CVE-2023-42917, involves memory corruption, giving attackers the capability to execute arbitrary code on targeted devices. This occurs after enticing victims to access specially crafted web content.

#3

It is noteworthy to highlight that all third-party web browsers available for iOS and iPadOS, such as Google Chrome, Mozilla Firefox, Microsoft Edge, and others, utilize the WebKit rendering engine, creating a lucrative and extensive attack surface.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-42916	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	cpe:2.3:a:apple:safari:*:*:*:*:*:*	CWE-125
CVE-2023-42917		cpe:2.3:o:apple:ipados:*:*:*:*:*:*	CWE-787
		cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*	
		cpe:2.3:o:apple:macos:*:*:*:*:*:*	

Recommendations



Update Software: Apply the latest security updates provided by Apple to remediate the vulnerabilities (CVE-2023-42916 and CVE-2023-42917), as keeping software up to date is crucial for maintaining the security and integrity of Apple devices.



User Vigilance: Exercise caution when interacting with web content, especially if it appears suspicious or is from unfamiliar sources. Be mindful of potential phishing attempts or malicious websites that could exploit the identified flaws.



Review and Adjust Browser Security Settings: Evaluate and adjust browser security settings on Apple devices to ensure an optimal balance between usability and security. Consider disabling unnecessary features that may expose devices to potential risks.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0009</u> Collection	<u>T1588</u> Obtain Capabilities
<u>T1204</u> User Execution	<u>T1059</u> Command and Scripting Interpreter	<u>T1213</u> Data from Information Repositories	<u>T1588.006</u> Vulnerabilities
<u>T1588.005</u> Exploits			

Patch Details

Ensure your Apple devices are shielded from cyber threats by promptly updating to the latest software versions. Apple has swiftly responded to the identified vulnerabilities, providing patches through the release of iOS 17.1.2, iPadOS 17.1.2, macOS Sonoma 14.1.2, and Safari 17.1.2.

Links:

<https://support.apple.com/en-us/HT214031>

<https://support.apple.com/en-us/HT214032>

<https://support.apple.com/en-us/HT214033>

References

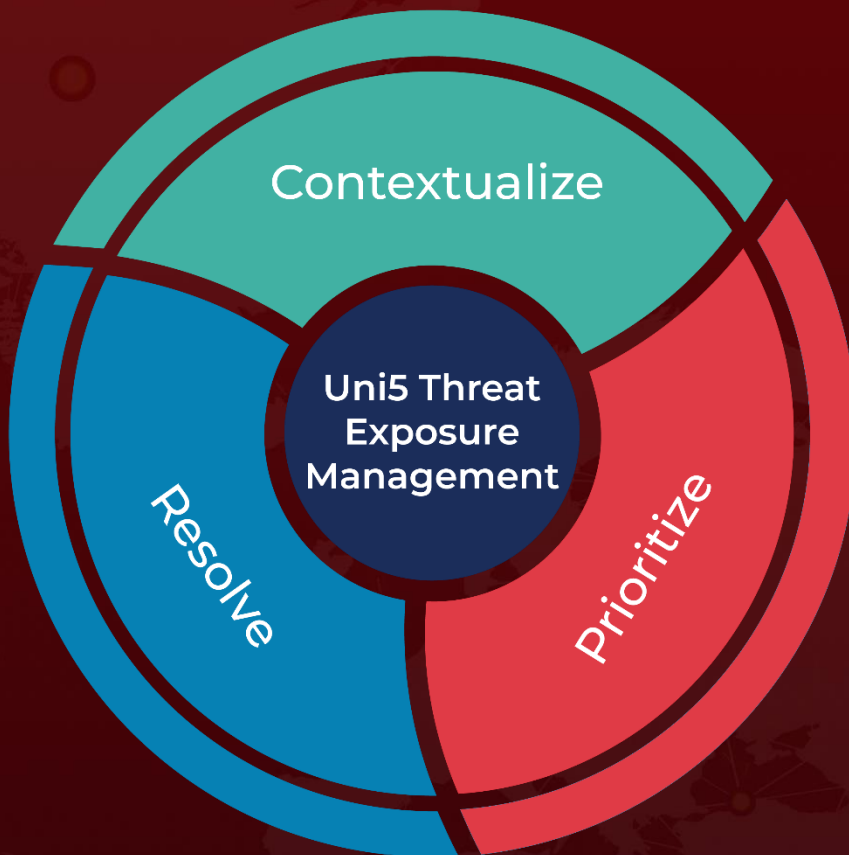
<https://socradar.io/apple-addresses-exploited-zero-day-vulnerabilities-with-emergency-security-update-cve-2023-42916-cve-2023-42917/>

<https://www.cisa.gov/news-events/alerts/2023/12/04/cisa-adds-two-known-exploited-vulnerabilities-catalog>

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

December 13, 2023 • 5:00 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com