Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Apple Addresses A Zero-Day Vulnerability Which Is Actively Exploited in Wild

Date of Publication	Admiralty Code	TA Number
July 11, 2023	A1	TA2023293

Summary

First Seen: July 10, 2023
Affected Platforms: Apple Safari, Apple iOS, Apple iPadOS, Apple macOS
Impact: The zero-day vulnerability (CVE-2023-37450) discovered in multiple Apple products is being actively exploited in the wild, specifically when processing web content. This vulnerability can potentially result in arbitrary code execution.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-37450	Apple WebKit Remote Code Execution Vulnerability	Apple Safari Apple iOS Apple iPadOS Apple macOS	✓	✗	✓

Vulnerability Details

#1

Apple has released Rapid Security Response updates for iOS, iPadOS, macOS, and Safari web browser to fix a zero-day vulnerability that has been actively exploited. The vulnerability, identified as CVE-2023-37450, could allow attackers to execute arbitrary code by using specially crafted web content. The flaw was discovered and reported by an anonymous researcher. Apple has addressed a total of 10 zero-day vulnerabilities since the beginning of 2023.

#2

However, the software update was pulled after reports that it caused errors on certain websites like Facebook, Instagram, and Zoom. The updates include patches for fully-patched iPhones, Macs, and iPads, and they are recommended for all users. The vulnerability affects the WebKit browser engine developed by Apple, and the company has implemented improved checks to prevent exploitation attempts.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-37450	Apple Safari up to 16.5.2 Apple iOS and iPadOS up to 16.5.1 Apple macOS up to 13.4.1.	cpe:2.3:a:apple:safari:16.5.0:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:16.5.1:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:16.5.2:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:16.5.0:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:16.5.1:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:16.5.0:*:*:*:*:*:*:* cpe:2.3:o:apple:mac_os:13.4.0:*:*:*:*:*:*:* cpe:2.3:o:apple:mac_os:13.4.1:*:*:*:*:*:*:*	CWE-94

Recommendations

Install the Rapid Security Response (RSR) updates: Ensure that you have the latest RSR updates installed on your iOS, iPadOS, macOS, and Safari web browser. These updates address the zero-day vulnerability and provide important security fixes. If you have automatic updates enabled, the patches will be applied automatically. Otherwise, manually install the updates as soon as they are available.

Verify the installed versions: Check the version numbers of your operating systems and Safari web browser to ensure they match the latest releases: iOS 16.5.1 (a), iPadOS 16.5.1 (a), macOS Ventura 13.4.1 (a), and Safari 16.5.2. If your versions do not match, update immediately.

Remain vigilant: Since the vulnerability was actively exploited, it's essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0040 Impact
T1189 Drive-by Compromise	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits
T1203 Exploitation for Client Execution	T1204 User Execution	T1204.001 Malicious Link	

Patch Details

https://support.apple.com/en-gb/HT213826

https://support.apple.com/en-gb/HT213823

https://support.apple.com/en-gb/HT213825

References

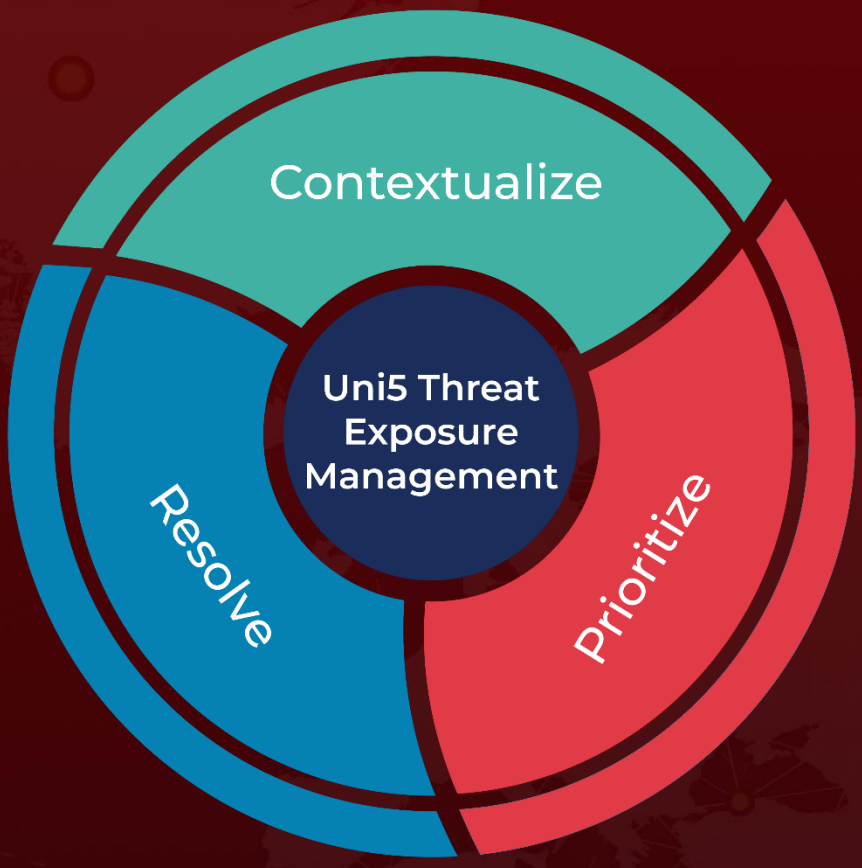
https://support.apple.com/en-us/HT201222

https://thehackernews.com/2023/07/apple-issues-urgent-patch-for-zero-day.html

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 11, 2023 • 4:30 AM

More at www.hivepro.com