Apple Fixes New Webkit Zero-Day Exploited to Hack Iphones, Macs

Severity: High

Date: 16th Feb 2023

Description

Apple has released emergency security updates to address a new zero-day vulnerability used in attacks to hack iPhones, iPads, and Macs.

The zero-day patched today is tracked as CVE-2023-23529 and is a WebKit confusion issue that could be exploited to trigger OS crashes and gain code execution on compromised devices.

Impact

Successful exploitation enables attackers to execute arbitrary code on devices running vulnerable iOS, iPadOS, and macOS versions after opening a malicious web page (the bug also impacts Safari 16.3.1 on macOS Big Sur and Monterey).

Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Apple addressed CVE-2023-23529 with improved checks in iOS 16.3.1, iPadOS 16.3.1, and macOS Ventura 13.2.1. The company also fixed CVE-2023-23514, that resides in the kernel. The vulnerability was addressed with improved memory management.

The complete list of impacted devices is quite extensive, as the bug affects older and newer models, and it includes.

- iPhone 8 and later
- iPad Pro (all models), iPad Air 3rd generation and later, iPad 5th generation and later, and iPad mini 5th generation and later
- Macs running macOS Ventura

Fix

By restricting access to this information, Apple likely wants to allow as many users as possible to update their devices before more attackers pick up on the zero-day's details to develop and deploy their own custom exploits targeting vulnerable iPhones, iPads, and Macs.

While this zero-day bug was likely used in targeted attacks, highly recommended to install emergency updates to block potential attack attempts.

Reference Links

https://www.bleepingcomputer.com/news/apple/apple-fixes-actively-exploited-ios-zero-day-on-older-iphones-ipads/

https://securityaffairs.com/142200/hacking/apple-zero-day-iphones-macs.html