Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Apple Zero Day Vulnerabilities

Date of Issue: 24 August 2022

Affected Systems:

- Macs running macOS Monterey
- iPhone 6s and later
- iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation).

Severity Level: High

Description

Apple has released a security update fixing two zero-day common vulnerability and exposures (CVE) that they state are being actively exploited. It is unknown as to how these bugs were discovered outside of the reports from an anonymous researcher. The exploits can grant an attacker remote code execution (RCE) and kernel level privileges on a device. A device compromised from these exploits could be subjected to data access to an unauthorized user, location retrieval, internet tracking, and much more.

CERT-MU strongly encourages users to update their Apple devices immediately.

Technical Information

Two zero day vulnerabilities have been reported in Apple devices and they could be exploited by remote attackers to execute arbitrary code and ultimately take over devices. One of the flaws is a kernel bug (CVE-2022-32894), which is present both in iOS and macOS. According to Apple it is an "out-of-bounds" write issue that was addressed with improved bounds checking. The vulnerability allows an application to execute arbitrary code with kernel privileges.

The second flaw is identified as a WebKit bug (CVE-2022-32893), which is an out-of-bounds write issue that Apple addressed with improved bounds checking. The flaw allows for processing maliciously crafted web content that can lead to code execution, and also has been reported to be under active exploit, according to Apple. WebKit is the browser engine that powers Safari and all other third-party browsers that work on iOS.

Workaround

Apple has already published advisories for the vulnerabilities on their webpage. Users are strongly advised to update their apple devices.

To update your device:

On iPhone or iPad: Settings > General > Software Update
On Mac: Apple menu > About this Mac > Software Update

More information about the update is available on:
https://support.apple.com/en-us/HT213412

Report Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication and Innovation
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info: contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org