Security Advisory 2024-025

Zero-Day Vulnerabilities in Apple Products

March 6, 2024 — v1.0

TLP:CLEAR

History:

- *06/03/2024 — v1.0 – Initial publication*

Summary

On March 5, 2024, Apple released new product versions providing fixes for several vulnerabilities affecting iOS and iPadOS, among which 2 zero-day vulnerabilities already exploited in the wild.

It is recommended updating as soon as possible.

Technical Details

The two zero-day vulnerabilities, namely `CVE-2024-23225` and `CVE-2024-23296`, respectively exist in the iOS Kernel and RTKit. A memory corruption in those components would allow an attacker with arbitrary kernel read and write capability to bypass kernel memory protections.

Affected Products

The list of impacted Apple devices includes:

- iPhone XS and later;
- iPhone 8, iPhone 8 Plus;
- iPhone X, iPad 5th generation;
- iPad Pro 9.7-inch;
- iPad Pro 12.9-inch 1st generation;
- 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

Recommendations

CERT-EU strongly recommends updating affected devices as soon as possible.

References

[1] https://support.apple.com/en-us/HT214081