Security Advisory 2023-069

Zero-Day Vulnerabilities in Apple Products

October 6, 2023 — v1.1

TLP:CLEAR

History:

- *25/09/2023 — v1.0 – Initial publication*
- *06/10/2023 — v1.1 – Updated with new emergency patch*

Summary

On September 21, Apple issued emergency patches for three zero-day bugs, identified by `CVE-2023-41992`, `CVE-2023-41991` and `CVE-2023-41993`. These vulnerabilities are affecting iOS, iPadOS, and macOS devices and are currently being used in the wild for spyware installation purposes [1].

Updates as of 06/10/2023 Apple released another emergency update to patch a new zero-day flaw tracked as `CVE-2023-42824` and reported to be exploited against version of iOS before 16.6. This update also fixes `CVE-2023-5217`, a buffer overflow in `libpvx` that may result in arbitrary code execution.

Updating is recommended as soon as possible.

Technical Details

The vulnerabilities `CVE-2023-41993` and `CVE-2023-41991` were found respectively in the WebKit browser engine and the Security framework. They could allow attackers to bypass signature validation using malicious apps or gain arbitrary code execution via maliciously crafted web pages.

Regarding the vulnerability `CVE-2023-41992`, it was found in the Kernel Framework, which provides APIs and support for kernel extensions and kernel-resident device drivers. Local attackers can exploit this flaw to escalate privileges.

Updates as of 06/10/2023 `CVE-2023-42824` is related to a weakness in the XNU kernel and can be exploited to escalate privileges as well.

Affected Products

The list of impacted devices encompasses older and newer device models, and it includes:

- iPhone 8 and later;
- iPad mini 5th generation and later;
- Macs running macOS Monterey and newer;
- Apple Watch Series 4 and later.

Recommendations

This issue is fixed in iOS 16.7 and iPadOS 16.7, iOS 17.0.1 and iPadOS 17.0.1, watchOS 9.6.3, macOS Ventura 13.6, watchOS 10.0.1. Any other version can be considered as vulnerable.

Updates as on 06/10/2023 Both `CVE-2023-42824` and `CVE-2023-5217` are fixed in iOS 17.0.3 and iPadOS 17.0.3.

CERT-EU strongly recommends that all devices running a version affected by the issues described above are upgraded to the latest version as soon as possible.

References

[1] https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

[2] https://support.apple.com/en-us/HT213926

[3] https://support.apple.com/en-us/HT213931

[4] https://support.apple.com/en-us/HT213961