Zero-Day Vulnerability in Apple Products

January 24, 2024 — v1.0

TLP:CLEAR

History:

- *24/01/2024 — v1.0 – Initial publication*

Summary

On January 22, 20024, Apple issued updates for a zero-day vulnerability identified as `CVE-2024-23222` [1]. This vulnerability affects iOS, iPadOS, macOS and tvOS devices and is currently being exploited in the wild [2]. The updates also contain fixes for other vulnerabilities affecting Apple products.

It is recommended updating as soon as possible.

Technical Details

The vulnerability `CVE-2024-23222` exists in the WebKit browser engine, and is due to a type confusion. It could allow attackers to execute arbitrary code on an affected device after opening a maliciously crafted web page.

Affected Products

- macOS 12.x before 12.7, 13.x before 13.6, 14.x before 14.3;
- iOS and iPadOS 16.x before 16.7, 17.x before 17.3;
- tvOS before 17.3;
- Safari before 17.3.

Recommendations

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

References

[1] https://www.cve.org/CVERecord?id=CVE-2024-23222

[2] https://support.apple.com/en-us/HT214061

[3] https://support.apple.com/en-us/HT214059

[4] https://support.apple.com/en-us/HT214063

[5] https://support.apple.com/en-us/HT214055

[6] https://support.apple.com/en-us/HT214056

[7] https://support.apple.com/en-us/HT214058

[8] https://support.apple.com/en-us/HT214057