Security for the greater good

Newscast

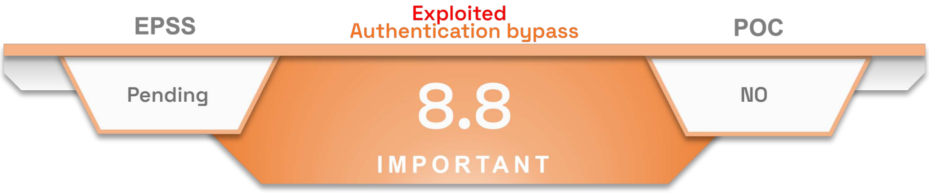
Critical vulnerability in Apple

2024-02-01 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

Apple - CVE-2022-48618



On 13 december 2022, Apple published a security advisory for their following products: *iOS*, *iPadOS*, *macOS* (*Ventura*), *watchOS* and *tvOS*.

These security updates address the vulnerability CVE-2022-48618 made public on January 9, 2024.

This vulnerability is due to a control flaw in the Apple Kernel. An attacker with read and write access rights can bypass *Pointer Authentication*.

⚠ | This vulnerability is exploited.

🔥 | CISA added this vulnerability to its *Known Exploited Vulnerabilities (KEV)* database on 31 January 2024.

Type of vulnerability

- **CWE-287** : Improper Authentication

Risk

- Authentication bypass

Severity (base score CVSS 3.1)

Attack vector	Local	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- iOS et iPadOS versions prior to 16.2
- macOS Ventura versions prior to 13.1
- tvOS versions prior to 16.2
- watchOS versions prior to 9.2

Recommendations

- Update iOS et iPadOS to versions 16.2 or later.
- Update macOS Ventura to version 13.1 or later.
- Update tvOS to version 16.2 or later.
- Update watchOS to version 9.2 or later.
- Additional information is available in Apple's security advisory.

Proof of concept

To date, no proof of concept is available in open source.

Sources

- https://www.cve.org/CVERecord?id=CVE-2022-48618
- https://support.apple.com/en-us/HT213530
- https://support.apple.com/en-us/HT213532
- https://support.apple.com/en-us/HT213535
- https://support.apple.com/en-us/HT213536