

# About the security content of visionOS 2.5

This document describes the security content of visionOS 2.5.

## About Apple security updates

For our customers' protection, Apple doesn't disclose, discuss, or confirm security issues until an investigation has occurred and patches or releases are available. Recent releases are listed on the [Apple security releases](#) page.

Apple security documents reference vulnerabilities by [CVE-ID](#) when possible.

For more information about security, see the [Apple Product Security](#) page.

## visionOS 2.5

Released May 12, 2025

### AppleJPEG

Available for: Apple Vision Pro

Impact: Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory

Description: The issue was addressed with improved input sanitization.

CVE-2025-31251: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

### Core Bluetooth

Available for: Apple Vision Pro

Impact: An app may be able to access sensitive user data

Description: This issue was addressed through improved state management.

CVE-2025-31212: Guilherme Rambo of Best Buddy Apps (rambo.codes)

### CoreAudio

Available for: Apple Vision Pro

Impact: Parsing a file may lead to an unexpected app termination

Description: The issue was addressed with improved checks.

CVE-2025-31208: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

### CoreGraphics

Available for: Apple Vision Pro

Impact: Parsing a file may lead to disclosure of user information

Description: An out-of-bounds read was addressed with improved bounds checking.

CVE-2025-31209: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

## **CoreMedia**

Available for: Apple Vision Pro

Impact: Parsing a file may lead to an unexpected app termination

Description: A use-after-free issue was addressed with improved memory management.

CVE-2025-31239: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

## **CoreMedia**

Available for: Apple Vision Pro

Impact: Processing a maliciously crafted video file may lead to unexpected app termination or corrupt process memory

Description: The issue was addressed with improved input sanitization.

CVE-2025-31233: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

## **iCloud Document Sharing**

Available for: Apple Vision Pro

Impact: An attacker may be able to turn on sharing of an iCloud folder without authentication

Description: This issue was addressed with additional entitlement checks.

CVE-2025-30448: Dayton Pidhirney of Atredis Partners, Lyutoon and YenKoc

## **ImageIO**

Available for: Apple Vision Pro

Impact: Processing a maliciously crafted image may lead to a denial-of-service

Description: A logic issue was addressed with improved checks.

CVE-2025-31226: Saagar Jha

## **Kernel**

Available for: Apple Vision Pro

Impact: An attacker may be able to cause unexpected system termination or corrupt kernel memory

Description: The issue was addressed with improved memory handling.

CVE-2025-31219: Michael DePlante (@izobashi) and Lucas Leong (@\_wmliang\_) of Trend Micro Zero Day Initiative

## **Kernel**

Available for: Apple Vision Pro

Impact: A remote attacker may cause an unexpected app termination

Description: A double free issue was addressed with improved memory management.

CVE-2025-31241: Christian Kohlschütter

## **libexpat**

Available for: Apple Vision Pro

Impact: Multiple issues in libexpat, including unexpected app termination or arbitrary code execution

Description: This is a vulnerability in open source code and Apple Software is among the affected projects. The CVE-ID was assigned by a third party. Learn more about the issue and CVE-ID at [cve.org](https://cve.org).

CVE-2024-8176

## **mDNSResponder**

Available for: Apple Vision Pro

Impact: A user may be able to elevate privileges

Description: A correctness issue was addressed with improved checks.

CVE-2025-31222: Paweł Płatek (Trail of Bits)

## **Pro Res**

Available for: Apple Vision Pro

Impact: An app may be able to cause unexpected system termination

Description: The issue was addressed with improved checks.

CVE-2025-31245: wac

## **Pro Res**

Available for: Apple Vision Pro

Impact: An attacker may be able to cause unexpected system termination or corrupt kernel memory

Description: The issue was addressed with improved input sanitization.

CVE-2025-31234: CertiK (@CertiK)

## **Security**

Available for: Apple Vision Pro

Impact: A remote attacker may be able to leak memory

Description: An integer overflow was addressed with improved input validation.

CVE-2025-31221: Dave G.

## WebKit

Available for: Apple Vision Pro

Impact: A type confusion issue could lead to memory corruption

Description: This issue was addressed with improved handling of floats.

WebKit Bugzilla: 286694

CVE-2025-24213: Google V8 Security Team

## WebKit

Available for: Apple Vision Pro

Impact: Processing maliciously crafted web content may lead to memory corruption

Description: The issue was addressed with improved checks.

WebKit Bugzilla: 289387

CVE-2025-31223: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

WebKit Bugzilla: 289653

CVE-2025-31238: was working with Trend Micro Zero Day Initiative

## WebKit

Available for: Apple Vision Pro

Impact: Processing maliciously crafted web content may lead to memory corruption

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 287577

CVE-2025-24223: rheza (@ginggilBesel) and an anonymous researcher

WebKit Bugzilla: 291506

CVE-2025-31204: Nan Wang (@eternalsakura13)

## WebKit

Available for: Apple Vision Pro

Impact: Processing maliciously crafted web content may lead to an unexpected Safari crash

Description: The issue was addressed with improved input validation.

WebKit Bugzilla: 289677

CVE-2025-31217: Ignacio Sanmillan (@ulexec)

## WebKit

Available for: Apple Vision Pro

Impact: Processing maliciously crafted web content may lead to an unexpected process crash

Description: The issue was addressed with improved checks.

WebKit Bugzilla: 288814

CVE-2025-31215: Jiming Wang and Jikai Ren

## WebKit

Available for: Apple Vision Pro

Impact: Processing maliciously crafted web content may lead to an unexpected Safari crash

Description: A type confusion issue was addressed with improved state handling.

WebKit Bugzilla: 290834

CVE-2025-31206: an anonymous researcher

## WebKit

Available for: Apple Vision Pro

Impact: A malicious website may exfiltrate data cross-origin

Description: The issue was addressed with improved checks.

WebKit Bugzilla: 290992

CVE-2025-31205: Ivan Fratric of Google Project Zero

## WebKit

Available for: Apple Vision Pro

Impact: Processing maliciously crafted web content may lead to an unexpected Safari crash

Description: This issue was addressed with improved memory handling.

WebKit Bugzilla: 290985

CVE-2025-31257: Juergen Schmied of Lynck GmbH

# Additional recognition

## AirDrop

We would like to acknowledge Dalibor Milanovic for their assistance.

## Kernel

We would like to acknowledge an anonymous researcher for their assistance.

## libnetcore

We would like to acknowledge Hoffcona of ByteDance IES Red Team for their assistance.

## MobileGestalt

We would like to acknowledge iisBuri for their assistance.

## NetworkExtension

We would like to acknowledge Andrei-Alexandru Bleorțu for their assistance.

## Safari

We would like to acknowledge Akash Labade, Narendra Bhati, Manager of Cyber Security at Suma Soft Pvt. Ltd, Pune (India) for their assistance.

## Shortcuts

We would like to acknowledge Candace Jensen of Kandji, Chi Yuan Chang of ZUSO ART and taikosoup, Egor Filatov (Positive Technologies), Monnier Pascaud for their assistance.

## WebKit

We would like to acknowledge Mike Dougherty and Daniel White of Google Chrome and an anonymous researcher for their assistance.

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. [Contact the vendor](#) for additional information.

Published Date: May 12, 2025

Helpful?

Yes

No

Support

About the security content of visionOS 2.5