About the security content of visionOS 2.4

This document describes the security content of visionOS 2.4.

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 2.4

Released March 31, 2025

Accounts

Available for: Apple Vision Pro

Impact: Sensitive keychain data may be accessible from an iOS backup

Description: This issue was addressed with improved data access restriction.

CVE-2025-24221: Lehan Dilusha @zorrosign Sri Lanka, and an anonymous researcher

AirPlay

Available for: Apple Vision Pro

Impact: An attacker on the local network may be able to cause a denial-of-service

Description: A null pointer dereference was addressed with improved input validation.

CVE-2025-31202: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple Vision Pro

Impact: An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without pairing

Description: An access issue was addressed with improved access restrictions.

CVE-2025-24271: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple Vision Pro

Impact: An attacker on the local network may be able to leak sensitive user information

Description: This issue was addressed by removing the vulnerable code.

CVE-2025-24270: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple Vision Pro

Impact: An attacker on the local network may be able to corrupt process memory

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

CVE-2025-24252: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple Vision Pro

Impact: An attacker on the local network may cause an unexpected app termination

Description: The issue was addressed with improved checks.

CVE-2025-24251: Uri Katz (Oligo Security)

CVE-2025-31197: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple Vision Pro

Impact: An attacker on the local network may be able to bypass authentication policy

Description: An authentication issue was addressed with improved state management.

CVE-2025-24206: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple Vision Pro

Impact: An attacker on the local network may cause an unexpected app termination

Description: A type confusion issue was addressed with improved checks.

CVE-2025-30445: Uri Katz (Oligo Security)

Entry added April 28, 2025

Audio

Available for: Apple Vision Pro

Impact: Processing a maliciously crafted file may lead to arbitrary code execution

Description: The issue was addressed with improved memory handling.

CVE-2025-24243: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

Authentication Services

Available for: Apple Vision Pro

Impact: Password autofill may fill in passwords after failing authentication

Description: This issue was addressed through improved state management.

CVE-2025-30430: Dominik Rath

Authentication Services

Available for: Apple Vision Pro

Impact: A malicious website may be able to claim WebAuthn credentials from another website that shares a registrable suffix

Description: The issue was addressed with improved input validation.

CVE-2025-24180: Martin Kreichgauer of Google Chrome

BiometricKit

Available for: Apple Vision Pro

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

Description: A buffer overflow was addressed with improved bounds checking.

CVE-2025-24237: Yutong Xiu

Calendar

Available for: Apple Vision Pro

Impact: An app may be able to break out of its sandbox

Description: A path handling issue was addressed with improved validation.

CVE-2025-30429: Denis Tokarev (@illusionofcha0s)

Calendar

Available for: Apple Vision Pro

Impact: An app may be able to break out of its sandbox

Description: This issue was addressed with improved checks.

CVE-2025-24212: Denis Tokarev (@illusionofcha0s)

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-2025-24163: Google Threat Analysis Group

CoreAudio

Available for: Apple Vision Pro

Impact: Playing a malicious audio file may lead to an unexpected app termination

Description: An out-of-bounds read issue was addressed with improved input validation.

CVE-2025-24230: 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: This issue was addressed with improved memory handling.

CVE-2025-24211: 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 memory handling.

CVE-2025-24190: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreText

Available for: Apple Vision Pro

Impact: Processing a maliciously crafted font may result in the disclosure of process memory

Description: An out-of-bounds read issue was addressed with improved input validation.

CVE-2025-24182: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreUtils

Available for: Apple Vision Pro

Impact: An attacker on the local network may be able to cause a denial-of-service

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

CVE-2025-31203: Uri Katz (Oligo Security)

Entry added April 28, 2025

curl

Available for: Apple Vision Pro

Impact: An input validation issue was addressed

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.

CVE-2024-9681

Focus

Available for: Apple Vision Pro

Impact: An attacker with physical access to a locked device may be able to view sensitive user information

Description: The issue was addressed with improved checks.

CVE-2025-30439: Andr.Ess

Focus

Available for: Apple Vision Pro

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

Description: A logging issue was addressed with improved data redaction.

CVE-2025-24283: Kirin (@Pwnrin)

Foundation

Available for: Apple Vision Pro

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

Description: The issue was resolved by sanitizing logging

CVE-2025-30447: LFY@secsys from Fudan University

ImageIO

Available for: Apple Vision Pro

Impact: Parsing an image may lead to disclosure of user information

Description: A logic error was addressed with improved error handling.

CVE-2025-24210: Anonymous working with Trend Micro Zero Day Initiative

IOGPUFamily

Available for: Apple Vision Pro

Impact: An app may be able to cause unexpected system termination or write kernel memory

Description: An out-of-bounds write issue was addressed with improved input validation.

CVE-2025-24257: Wang Yu of Cyberserval

Kernel

Available for: Apple Vision Pro

Impact: A malicious app may be able to attempt passcode entries on a locked device and thereby cause escalating time delays after 4 failures

Description: A logic issue was addressed with improved state management.

CVE-2025-30432: Michael (Biscuit) Thomas - @biscuit@social.lol

libarchive

Available for: Apple Vision Pro

Impact: An input validation issue was addressed

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.

CVE-2024-48958

libnetcore

Available for: Apple Vision Pro

Impact: Processing maliciously crafted web content may result in the disclosure of process memory

Description: A logic issue was addressed with improved checks.

CVE-2025-24194: an anonymous researcher

libxml2

Available for: Apple Vision Pro

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

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.

CVE-2025-27113

CVE-2024-56171

libxpc

Available for: Apple Vision Pro

Impact: An app may be able to delete files for which it does not have permission

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

CVE-2025-31182: Alex Radocea and Dave G. of Supernetworks, 风沐云烟(@binary_fmyy) and Minghao Lin(@Y1nKoc)

Maps

Available for: Apple Vision Pro

Impact: An app may be able to read sensitive location information

Description: A path handling issue was addressed with improved logic.

CVE-2025-30470: LFY@secsys from Fudan University

NetworkExtension

Available for: Apple Vision Pro

Impact: An app may be able to enumerate a user's installed apps

Description: This issue was addressed with additional entitlement checks.

CVE-2025-30426: Jimmy

Power Services

Available for: Apple Vision Pro

Impact: An app may be able to break out of its sandbox

Description: This issue was addressed with additional entitlement checks.

CVE-2025-24173: Mickey Jin (@patch1t)

RepairKit

Available for: Apple Vision Pro

Impact: An app may be able to bypass Privacy preferences

Description: This issue was addressed with additional entitlement checks.

CVE-2025-24095: Mickey Jin (@patch1t)

Safari

Available for: Apple Vision Pro

Impact: Visiting a malicious website may lead to user interface spoofing

Description: The issue was addressed with improved UI.

CVE-2025-24113: @RenwaX23

Security

Available for: Apple Vision Pro

Impact: A remote user may be able to cause a denial-of-service

Description: A validation issue was addressed with improved logic.

CVE-2025-30471: Bing Shi, Wenchao Li, Xiaolong Bai of Alibaba Group, Luyi Xing of Indiana University Bloomington

Share Sheet

Available for: Apple Vision Pro

Impact: A malicious app may be able to dismiss the system notification on the Lock Screen that a recording was started

Description: This issue was addressed with improved access restrictions.

CVE-2025-30438: Halle Winkler, Politepix theoffcuts.org

Shortcuts

Available for: Apple Vision Pro

Impact: A shortcut may be able to access files that are normally inaccessible to the Shortcuts app

Description: This issue was addressed with improved access restrictions.

CVE-2025-30433: Andrew James Gonzalez

Siri

Available for: Apple Vision Pro

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

Description: A privacy issue was addressed by not logging contents of text fields.

CVE-2025-24214: Kirin (@Pwnrin)

Web Extensions

Available for: Apple Vision Pro

Impact: An app may gain unauthorized access to Local Network

Description: This issue was addressed with improved permissions checking.

CVE-2025-31184: Alexander Heinrich (@Sn0wfreeze), SEEMOO, TU Darmstadt & Mathy Vanhoef (@vanhoefm) and Jeroen Robben (@RobbenJeroen), DistriNet, KU Leuven

Web Extensions

Available for: Apple Vision Pro

Impact: Visiting a website may leak sensitive data

Description: A script imports issue was addressed with improved isolation.

CVE-2025-24192: Vsevolod Kokorin (Slonser) of Solidlab

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 memory handling.

WebKit Bugzilla: 285892

CVE-2025-24264: Gary Kwong, and an anonymous researcher

WebKit Bugzilla: 284055

CVE-2025-24216: Paul Bakker of ParagonERP

WebKit

Available for: Apple Vision Pro

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

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

WebKit Bugzilla: 285643

CVE-2025-30427: rheza (@ginggilBesel)

Additional recognition

Accessibility

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) of Lakshmi Narain College of Technology Bhopal India, Richard Hyunho Im (@richeeta) with routezero.security for their assistance.

AirPlay

We would like to acknowledge Uri Katz (Oligo Security) for their assistance.

Entry added April 28, 2025

Apple Account

We would like to acknowledge Byron Fecho for their assistance.

Audio

We would like to acknowledge Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative for their assistance.

FaceTime

We would like to acknowledge Anonymous, Dohyun Lee (@l33d0hyun) of USELab, Korea University & Youngho Choi of CEL, Korea University & Geumhwan Cho of USELab, Korea University for their assistance.

Find My

We would like to acknowledge 神罚(@Pwnrin) for their assistance.

Foundation

We would like to acknowledge Jann Horn of Google Project Zero for their assistance.

HearingCore

We would like to acknowledge Kirin@Pwnrin and LFY@secsys from Fudan University for their assistance.

ImageIO

We would like to acknowledge D4m0n for their assistance.

Mail

We would like to acknowledge Doria Tang, Ka Lok Wu, Prof. Sze Yiu Chau of The Chinese University of Hong Kong for their assistance.

Messages

We would like to acknowledge parkminchan from Korea Univ. for their assistance.

Photos

We would like to acknowledge Bistrit Dahal for their assistance.

Safari Extensions

We would like to acknowledge Alisha Ukani, Pete Snyder, Alex C. Snoeren for their assistance.

Sandbox Profiles

We would like to acknowledge Benjamin Hornbeck for their assistance.

SceneKit

We would like to acknowledge Marc Schoenefeld, Dr. rer. nat. for their assistance.

Security

We would like to acknowledge Kevin Jones (GitHub) for their assistance.

Settings

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) from C-DAC Thiruvananthapuram India for their assistance.

Shortcuts

We would like to acknowledge Chi Yuan Chang of ZUSO ART and taikosoup for their assistance.

WebKit

We would like to acknowledge Wai Kin Wong, Dongwei Xiao, Shuai Wang and Daoyuan Wu of HKUST Cybersecurity Lab, Anthony Lai(@darkfloyd1014) of VXRL, Wong Wai Kin, Dongwei Xiao and Shuai Wang of HKUST Cybersecurity Lab, Anthony Lai (@darkfloyd1014) of VXRL., Xiangwei Zhang of Tencent Security YUNDING LAB, and an anonymous researcher for their assistance.

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: April 29, 2025

Helpful? Yes No