About the security content of macOS Ventura 13.7.6

This document describes the security content of macOS Ventura 13.7.6.

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.

macOS Ventura 13.7.6

Released May 12, 2025

afpfs

Available for: macOS Ventura

Impact: Mounting a maliciously crafted AFP network share may lead to system termination

Description: This issue was addressed with improved checks.

CVE-2025-31240: Dave G.

CVE-2025-31237: Dave G.

AppleJPEG

Available for: macOS Ventura

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

Audio

Available for: macOS Ventura

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

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

CVE-2025-31235: Dillon Franke working with Google Project Zero

CoreAudio

Available for: macOS Ventura

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: macOS Ventura

Impact: Processing a maliciously crafted file may lead to a denial-of-service or potentially disclose memory contents

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

CVE-2025-31196: wac working with Trend Micro Zero Day Initiative

CoreGraphics

Available for: macOS Ventura

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: macOS Ventura

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: macOS Ventura

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

DiskArbitration

Available for: macOS Ventura

Impact: A malicious app may be able to gain root privileges

Description: The issue was addressed with additional permissions checks.

CVE-2025-30453: Csaba Fitzl (@theevilbit) of Kandji, an anonymous researcher

DiskArbitration

Available for: macOS Ventura

Impact: An app may be able to gain root privileges

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24258: Csaba Fitzl (@theevilbit) of Kandji, an anonymous researcher

iCloud Document Sharing

Available for: macOS Ventura

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

Installer

Available for: macOS Ventura

Impact: A sandboxed app may be able to access sensitive user data

Description: A logic issue was addressed with improved checks.

CVE-2025-31232: an anonymous researcher

Kernel

Available for: macOS Ventura

Impact: An app may be able to leak sensitive kernel state

Description: An information disclosure issue was addressed by removing the vulnerable code.

CVE-2025-24144: Mateusz Krzywicki (@krzywix)

Kernel

Available for: macOS Ventura

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: macOS Ventura

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: macOS Ventura

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.

CVE-2024-8176

Libinfo

Available for: macOS Ventura

Impact: An app may be able to bypass ASLR

Description: The issue was addressed with improved checks.

CVE-2025-30440: Paweł Płatek (Trail of Bits)

mDNSResponder

Available for: macOS Ventura

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)

Mobile Device Service

Available for: macOS Ventura

Impact: A malicious app may be able to gain root privileges

Description: An input validation issue was addressed by removing the vulnerable code.

CVE-2025-24274: an anonymous researcher

Notification Center

Available for: macOS Ventura

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

Description: A privacy issue was addressed with improved private data redaction for log entries.

CVE-2025-24142: LFY@secsys from Fudan University

Pro Res

Available for: macOS Ventura

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

Description: The issue was addressed with improved checks.

CVE-2025-31245: wac

Sandbox

Available for: macOS Ventura

Impact: An app may be able to bypass certain Privacy preferences

Description: A logic issue was addressed with improved checks.

CVE-2025-31224: Csaba Fitzl (@theevilbit) of Kandji

Security

Available for: macOS Ventura

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.

Security

Available for: macOS Ventura

Impact: An app may be able to access associated usernames and websites in a user's iCloud Keychain

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

CVE-2025-31213: Kirin (@Pwnrin) and 7feilee

SharedFileList

Available for: macOS Ventura

Impact: An attacker may gain access to protected parts of the file system

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

CVE-2025-31247: an anonymous researcher

SoftwareUpdate

Available for: macOS Ventura

Impact: An app may be able to gain elevated privileges

Description: The issue was addressed with improved input sanitization.

CVE-2025-30442: an anonymous researcher

StoreKit

Available for: macOS Ventura

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

Description: A privacy issue was addressed with improved private data redaction for log entries.

CVE-2025-31242: Eric Dorphy of Twin Cities App Dev LLC

Weather

Available for: macOS Ventura

Impact: A malicious app may be able to read sensitive location information

Description: A privacy issue was addressed by removing sensitive data.

CVE-2025-31220: Adam M.

WebContentFilter

Available for: macOS Ventura

Impact: An app may be able to disclose kernel memory

Description: The issue was addressed with improved memory handling.

CVE-2025-24155: an anonymous researcher

Additional recognition

Kernel

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

Published Date: May 12, 2025