About the security content of macOS Sonoma 14.7.7

This document describes the security content of macOS Sonoma 14.7.7.

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 Sonoma 14.7.7

Released July 29, 2025

Admin Framework

Available for: macOS Sonoma

Impact: An app may be able to cause a denial-of-service

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

CVE-2025-43191: Ryan Dowd (@_rdowd)

afclip

Available for: macOS Sonoma

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

Description: The issue was addressed with improved memory handling.

CVE-2025-43186: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

AMD

Available for: macOS Sonoma

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

Description: A race condition was addressed with improved state handling.

CVE-2025-43244: ABC Research s.r.o.

AppleMobileFileIntegrity

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-31243: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

Available for: macOS Sonoma

Impact: A malicious app may be able to launch arbitrary binaries on a trusted device

Description: This issue was addressed with improved input validation.

CVE-2025-43253: Noah Gregory (wts.dev)

AppleMobileFileIntegrity

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

Description: A logic issue was addressed with improved checks.

CVE-2025-43249: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

Available for: macOS Sonoma

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

Description: A logic issue was addressed with improved restrictions.

CVE-2025-43248: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

Available for: macOS Sonoma

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

Description: A downgrade issue was addressed with additional code-signing restrictions.

CVE-2025-43245: Mickey Jin (@patch1t)

CFNetwork

Available for: macOS Sonoma

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

Description: A use-after-free issue was addressed by removing the vulnerable code.

CVE-2025-43222: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

CFNetwork

Available for: macOS Sonoma

Impact: A non-privileged user may be able to modify restricted network settings

Description: A denial-of-service issue was addressed with improved input validation.

CVE-2025-43223: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

copyfile

Available for: macOS Sonoma

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

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

CVE-2025-43220: Mickey Jin (@patch1t)

CoreMedia

Available for: macOS Sonoma

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

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

CVE-2025-43210: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreServices

Available for: macOS Sonoma

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

Description: A permissions issue was addressed by removing the vulnerable code.

CVE-2025-43199: an anonymous researcher, Gergely Kalman (@gergely_kalman)

CoreServices

Available for: macOS Sonoma

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

Description: An issue existed in the handling of environment variables. This issue was addressed with improved validation.

CVE-2025-43195: 风沐云烟 (@binary_fmyy) and Minghao Lin (@Y1nKoc)

CoreServices

Available for: macOS Sonoma

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

Description: A logic issue was addressed with improved restrictions.

CVE-2025-43313: 风沐云烟@binary_fmyy

Entry added October 15, 2025

Disk Images

Available for: macOS Sonoma

Impact: Running an hdiutil command may unexpectedly execute arbitrary code

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

CVE-2025-43187: 风沐云烟 (@binary_fmyy) and Minghao Lin (@Y1nKoc)

Dock

Available for: macOS Sonoma

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

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

CVE-2025-43198: Mickey Jin (@patch1t)

file

Available for: macOS Sonoma

Impact: Processing a maliciously crafted file may lead to unexpected app termination

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

CVE-2025-43254: 2ourc3 | Salim Largo

File Bookmark

Available for: macOS Sonoma

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

Description: A logic issue was addressed with improved checks.

CVE-2025-43261: an anonymous researcher

Find My

Available for: macOS Sonoma

Impact: An app may be able to fingerprint the user

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-31279: Dawuge of Shuffle Team

Finder

Available for: macOS Sonoma

Impact: An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges

Description: This issue was addressed through improved state management.

CVE-2025-24119: an anonymous researcher

GPU Drivers

Available for: macOS Sonoma

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

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

CVE-2025-43255: Anonymous working with Trend Micro Zero Day Initiative

CVE-2025-43284: Anonymous working with Trend Micro Zero Day Initiative

Entry updated August 28, 2025

ICU

Available for: macOS Sonoma

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

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

CVE-2025-43209: Gary Kwong working with Trend Micro Zero Day Initiative

ImageIO

Available for: macOS Sonoma

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

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

CVE-2025-43226

Kernel

Available for: macOS Sonoma

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

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

CVE-2025-43282: Christian Kohlschütter

Entry added October 15, 2025

LaunchServices

Available for: macOS Sonoma

Impact: An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges

Description: This issue was addressed through improved state management.

CVE-2025-24119: an anonymous researcher

libxpc

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

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

CVE-2025-43196: an anonymous researcher

libxslt

Available for: macOS Sonoma

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

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-2025-7424: Ivan Fratric of Google Project Zero

Managed Configuration

Available for: macOS Sonoma

Impact: Account-driven User Enrollment may still be possible with Lockdown Mode turned on

Description: A configuration issue was addressed with additional restrictions.

CVE-2025-43192: Pyrophoria

NetAuth

Available for: macOS Sonoma

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

Description: A race condition was addressed with additional validation.

CVE-2025-43275: Csaba Fitzl (@theevilbit) of Kandji

Notes

Available for: macOS Sonoma

Impact: An app may gain unauthorized access to Local Network

Description: An access issue was addressed with additional sandbox restrictions.

CVE-2025-43270: Minghao Lin and Jiaxun Zhu

Entry updated October 15, 2025

Notes

Available for: macOS Sonoma

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

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

CVE-2025-43225: Kirin (@Pwnrin)

NSSpellChecker

Available for: macOS Sonoma

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-43266: Noah Gregory (wts.dev)

PackageKit

Available for: macOS Sonoma

Impact: An app may be able to hijack entitlements granted to other privileged apps

Description: This issue was addressed with improved data protection.

CVE-2025-43260: Zhongquan Li (@Guluisacat)

PackageKit

Available for: macOS Sonoma

Impact: A malicious app with root privileges may be able to modify the contents of system files

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-43247: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Sonoma

Impact: An app may be able to modify protected parts of the file system

Description: The issue was addressed with improved checks.

CVE-2025-43194: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Sonoma

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-43232: Koh M. Nakagawa (@tsunek0h), Csaba Fitzl (@theevilbit) of Kandji and Gergely Kalman (@gergely_kalman)

Power Management

Available for: macOS Sonoma

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

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

CVE-2025-43236: Dawuge of Shuffle Team

SceneKit

Available for: macOS Sonoma

Impact: An app may be able to read files outside of its sandbox

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-43241: Mickey Jin (@patch1t)

Security

Available for: macOS Sonoma

Impact: A malicious app acting as a HTTPS proxy could get access to sensitive user data

Description: This issue was addressed with improved access restrictions.

CVE-2025-43233: Wojciech Regula of SecuRing (wojciechregula.blog)

SecurityAgent

Available for: macOS Sonoma

Impact: An app may be able to cause a denial-of-service

Description: The issue was addressed with improved memory handling.

CVE-2025-43193: Dawuge of Shuffle Team

SharedFileList

Available for: macOS Sonoma

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

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

CVE-2025-43250: Yuebin Sun (@yuebinsun2020), Mickey Jin (@patch1t)

Shortcuts

Available for: macOS Sonoma

Impact: A shortcut may be able to bypass sensitive Shortcuts app settings

Description: This issue was addressed by adding an additional prompt for user consent.

CVE-2025-43184: Csaba Fitzl (@theevilbit) of Kandji

Single Sign-On

Available for: macOS Sonoma

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

Description: This issue was addressed with additional entitlement checks.

CVE-2025-43197: Shang-De Jiang and Kazma Ye of CyCraft Technology

sips

Available for: macOS Sonoma

Impact: Processing a maliciously crafted file may lead to unexpected app termination

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

CVE-2025-43239: Nikolai Skliarenko of Trend Micro Zero Day Initiative

Software Update

Available for: macOS Sonoma

Impact: An app may be able to modify protected parts of the file system

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-43243: Mickey Jin (@patch1t), Keith Yeo (@kyeojy) from Team Orca of Sea Security

Spotlight

Available for: macOS Sonoma

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

Description: This issue was addressed with improved checks.

CVE-2025-43246: Mickey Jin (@patch1t)

StorageKit

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

Description: This issue was addressed through improved state management.

CVE-2025-43256: an anonymous researcher

System Settings

Available for: macOS Sonoma

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

Description: A parsing issue in the handling of directory paths was addressed with improved path validation.

CVE-2025-43206: Zhongquan Li (@Guluisacat)

WebContentFilter

Available for: macOS Sonoma

Impact: A malicious app may be able to read kernel memory

Description: This issue was addressed with improved memory handling.

CVE-2025-43189: an anonymous researcher

WindowServer

Available for: macOS Sonoma

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

Description: This issue was addressed with improved redaction of sensitive information.

CVE-2025-43259: Martti Hütt

Xsan

Available for: macOS Sonoma

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

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

CVE-2025-43238: an anonymous researcher

Additional recognition

CoreAudio

We would like to acknowledge @zlluny, Noah Weinberg for their assistance.

Device Management

We would like to acknowledge Al Karak for their assistance.

Game Center

We would like to acknowledge YingQi Shi (@Mas0nShi) of DBAppSecurity's WeBin lab for their assistance.

libxslt

We would like to acknowledge Ivan Fratric of Google Project Zero for their assistance.

Shortcuts

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

WebDAV

We would like to acknowledge Christian Kohlschütter for their assistance.

Published Date: October 15, 2025