About the security content of macOS Sequoia 15.6

This document describes the security content of macOS Sequoia 15.6.

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 Sequoia 15.6

Released July 29, 2025

Admin Framework

Available for: macOS Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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)

Application Firewall

Available for: macOS Sequoia

Impact: A local attacker may be able to elevate their privileges

Description: The issue was addressed with improved authentication.

CVE-2025-43281: MRHAX, Aditya Rana

Entry added October 15, 2025

Archive Utility

Available for: macOS Sequoia

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

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

CVE-2025-43257: Mickey Jin (@patch1t)

CFNetwork

Available for: macOS Sequoia

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 Sequoia

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 Sequoia

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)

CoreAudio

Available for: macOS Sequoia

Impact: Processing a maliciously crafted audio file may lead to memory corruption

Description: The issue was addressed with improved memory handling.

CVE-2025-43277: Google's Threat Analysis Group

CoreMedia

Available for: macOS Sequoia

Impact: A sandboxed process may be able to circumvent sandbox restrictions

Description: A permissions issue was addressed with additional sandbox restrictions.

CVE-2025-43273: Seo Hyun-gyu (@wh1te4ever), Dora Orak, Minghao Lin (@Y1nKoc) and XiLong Zhang (@Resery4) of Xiaomi and noir (@ROIS) and fmyy (@风沐云烟)

CoreMedia

Available for: macOS Sequoia

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

CoreMedia Playback

Available for: macOS Sequoia

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

Description: The issue was addressed with additional permissions checks.

CVE-2025-43230: Chi Yuan Chang of ZUSO ART and taikosoup

CoreServices

Available for: macOS Sequoia

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)

Core Services

Available for: macOS Sequoia

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: Gergely Kalman (@gergely_kalman), an anonymous researcher

CoreServices

Available for: macOS Sequoia

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

Directory Utility

Available for: macOS Sequoia

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

Description: An injection issue was addressed with improved validation.

CVE-2025-43267: Mickey Jin (@patch1t)

Disk Images

Available for: macOS Sequoia

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)

DiskArbitration

Available for: macOS Sequoia

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-43188: an anonymous researcher

Dock

Available for: macOS Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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

GPU Drivers

Available for: macOS Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

Impact: iCloud Private Relay may not activate when more than one user is logged in at the same time

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

CVE-2025-43276: Willey Lin

Kernel

Available for: macOS Sequoia

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-43268: Gergely Kalman (@gergely_kalman), Arsenii Kostromin (0x3c3e)

Kernel

Available for: macOS Sequoia

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

libnetcore

Available for: macOS Sequoia

Impact: Processing a file may lead to memory corruption

Description: This issue was addressed with improved memory handling.

CVE-2025-43202: Brian Carpenter

libxml2

Available for: macOS Sequoia

Impact: Processing a file 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-2025-7425: Sergei Glazunov of Google Project Zero

libxpc

Available for: macOS Sequoia

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 Sequoia

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 Sequoia

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

MediaRemote

Available for: macOS Sequoia

Impact: A sandboxed process may be able to launch any installed app

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-31275: Dora Orak

Metal

Available for: macOS Sequoia

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

Description: Multiple memory corruption issues were addressed with improved input validation.

CVE-2025-43234: Vlad Stolyarov of Google's Threat Analysis Group

Model I/O

Available for: macOS Sequoia

Impact: Processing a maliciously crafted image may corrupt process memory

Description: The issue was addressed with improved memory handling.

CVE-2025-43264: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

CVE-2025-43219: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Model I/O

Available for: macOS Sequoia

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

Description: An input validation issue was addressed with improved memory handling.

CVE-2025-31281: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Model I/O

Available for: macOS Sequoia

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-2025-43224: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

CVE-2025-43221: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Model I/O

Available for: macOS Sequoia

Impact: Processing a maliciously crafted file may lead to heap corruption

Description: A memory corruption issue was addressed with improved validation.

CVE-2025-31280: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Model I/O

Available for: macOS Sequoia

Impact: Processing a maliciously crafted USD file may disclose memory contents

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

CVE-2025-43218: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Model I/O

Available for: macOS Sequoia

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

Description: The issue was addressed with improved checks.

CVE-2025-43215: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

NetAuth

Available for: macOS Sequoia

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 Sequoia

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)

Notes

Available for: macOS Sequoia

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

NSSpellChecker

Available for: macOS Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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

Power Management

Available for: macOS Sequoia

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

Description: The issue was addressed with improved memory handling.

CVE-2025-43235: Dawuge of Shuffle Team

RemoteViewServices

Available for: macOS Sequoia

Impact: A sandboxed process may be able to circumvent sandbox restrictions

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

CVE-2025-43274: an anonymous researcher, Hikerell of Loadshine Lab, @zlluny

Safari

Available for: macOS Sequoia

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

Description: A logic issue was addressed with improved checks.

CVE-2025-24188: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

SceneKit

Available for: macOS Sequoia

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 Sequoia

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 Sequoia

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 Sequoia

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: Mickey Jin (@patch1t), Yuebin Sun (@yuebinsun2020)

Single Sign-On

Available for: macOS Sequoia

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 Sequoia

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 Sequoia

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

Spotlight

Available for: macOS Sequoia

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)

SQLite

Available for: macOS Sequoia

Impact: Processing a file 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-2025-6965

Entry added October 15, 2025

StorageKit

Available for: macOS Sequoia

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 Sequoia

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)

User Management

Available for: macOS Sequoia

Impact: A local attacker may gain access to Keychain items

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

CVE-2025-43251: Mickey Jin (@patch1t)

Voice Control

Available for: macOS Sequoia

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

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

CVE-2025-43185: Mickey Jin (@patch1t)

WebContentFilter

Available for: macOS Sequoia

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

WebContentFilter

Available for: macOS Sequoia

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

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

CVE-2025-43237: an anonymous researcher

WebKit

Available for: macOS Sequoia

Impact: Processing maliciously crafted web content may lead to universal cross site scripting

Description: This issue was addressed through improved state management.

WebKit Bugzilla: 285927

CVE-2025-43229: Martin Bajanik of Fingerprint, Ammar Askar

WebKit

Available for: macOS Sequoia

Impact: Processing maliciously crafted web content may disclose sensitive user information

Description: This issue was addressed through improved state management.

WebKit Bugzilla: 292888

CVE-2025-43227: Gilad Moav, Yehuda Afek, Anat Bremler-Barr, and Amit Klein

Entry updated October 15, 2025

WebKit

Available for: macOS Sequoia

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

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 291742

CVE-2025-31278: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

WebKit Bugzilla: 291745

CVE-2025-31277: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

WebKit Bugzilla: 293579

CVE-2025-31273: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

WebKit

Available for: macOS Sequoia

Impact: A download's origin may be incorrectly associated

Description: A logic issue was addressed with improved checks.

WebKit Bugzilla: 293994

CVE-2025-43240: Syarif Muhammad Sajjad

WebKit

Available for: macOS Sequoia

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

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 292599

CVE-2025-43214: shandikri working with Trend Micro Zero Day Initiative, Google V8 Security Team

WebKit Bugzilla: 292621

CVE-2025-43213: Google V8 Security Team

WebKit Bugzilla: 293197

CVE-2025-43212: Nan Wang (@eternalsakura13) and Ziling Chen

WebKit

Available for: macOS Sequoia

Impact: Processing web content may lead to a denial-of-service

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 293730

CVE-2025-43211: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

WebKit

Available for: macOS Sequoia

Impact: Processing maliciously crafted web content may disclose internal states of the app

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

WebKit Bugzilla: 294182

CVE-2025-43265: HexRabbit (@h3xr4bb1t) from DEVCORE Research Team

WebKit

Available for: macOS Sequoia

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: 295382

CVE-2025-43216: Ignacio Sanmillan (@ulexec)

WebKit

Available for: macOS Sequoia

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

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.

WebKit Bugzilla: 296459

CVE-2025-6558: Clément Lecigne and Vlad Stolyarov of Google's Threat Analysis Group

WindowServer

Available for: macOS Sequoia

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 Sequoia

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

zip

Available for: macOS Sequoia

Impact: A website may be able to access sensitive user data when resolving symlinks

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

CVE-2025-43252: Jonathan Bar Or (@yo_yo_yo_jbo) of Microsoft

Additional recognition

AppleMobileFileIntegrity

We would like to acknowledge Mickey Jin (@patch1t) for their assistance.

Bluetooth

We would like to acknowledge LIdong LI, Xiao Wang, Shao Dong Chen, and Chao Tan of Source Guard for their assistance.

Control Center

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

CoreAudio

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

CoreUtils

We would like to acknowledge Csaba Fitzl (@theevilbit) of Kandji for their assistance.

Device Management

We would like to acknowledge Al Karak for their assistance.

Find My

We would like to acknowledge Christian Kohlschütter for their assistance.

Game Center

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

IOMobileFrameBuffer

We would like to acknowledge Karol Mazurek (@Karmaz95) of AFINE for their assistance.

Kernel

We would like to acknowledge Karol Mazurek (@Karmaz95) of AFINE for their assistance.

libxml2

We would like to acknowledge Sergei Glazunov of Google Project Zero for their assistance.

libxslt

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

Safari

We would like to acknowledge Ameen Basha M K for their assistance.

Shortcuts

We would like to acknowledge Dennis Kniep for their assistance.

WebDAV

We would like to acknowledge Christian Kohlschütter for their assistance.

WebKit

We would like to acknowledge Google V8 Security Team, Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei, rheza (@ginggilBesel) 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: October 15, 2025

Helpful? Yes No

Support About the security content of macOS Sequoia 15.6

Copyright © 2026 Apple Inc. All rights reserved. Privacy Policy | Terms of Use | Sales and Refunds | Site Map United States