About the security content of macOS Sequoia 15.4

This document describes the security content of macOS Sequoia 15.4.

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.

macOS Sequoia 15.4

Released March 31, 2025

Accessibility

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-2025-24202: Zhongcheng Li from IES Red Team of ByteDance

AccountPolicy

Available for: macOS Sequoia

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

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

CVE-2025-24234: an anonymous researcher

AirDrop

Available for: macOS Sequoia

Impact: An app may be able to read arbitrary file metadata

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24097: Ron Masas of BREAKPOINT.SH

AirPlay

Available for: macOS Sequoia

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: macOS Sequoia

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

AirPlay

Available for: macOS Sequoia

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: macOS Sequoia

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: macOS Sequoia

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: macOS Sequoia

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: macOS Sequoia

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

App Store

Available for: macOS Sequoia

Impact: A malicious app may be able to access private information

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

CVE-2025-24276: an anonymous researcher

AppleMobileFileIntegrity

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-2025-24272: 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-2025-24239: Wojciech Regula of SecuRing (wojciechregula.blog)

AppleMobileFileIntegrity

Available for: macOS Sequoia

Impact: A malicious app may be able to read or write to protected files

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24233: Claudio Bozzato and Francesco Benvenuto of Cisco Talos.

AppleMobileFileIntegrity

Available for: macOS Sequoia

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

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

CVE-2025-30443: Bohdan Stasiuk (@bohdan_stasiuk)

Audio

Available for: macOS Sequoia

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

Description: The issue was addressed with improved memory handling.

CVE-2025-24244: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

Audio

Available for: macOS Sequoia

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: macOS Sequoia

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: macOS Sequoia

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

Authentication Services

Available for: macOS Sequoia

Impact: A malicious app may be able to access a user's saved passwords

Description: This issue was addressed by adding a delay between verification code attempts.

CVE-2025-24245: Ian Mckay (@iann0036)

Automator

Available for: macOS Sequoia

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

Description: A permissions issue was addressed by removing vulnerable code and adding additional checks.

CVE-2025-30460: an anonymous researcher

BiometricKit

Available for: macOS Sequoia

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

Calendar

Available for: macOS Sequoia

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)

CloudKit

Available for: macOS Sequoia

Impact: A malicious app may be able to access private information

Description: The issue was addressed with improved checks.

CVE-2025-24215: Kirin (@Pwnrin)

CoreAudio

Available for: macOS Sequoia

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: macOS Sequoia

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: macOS Sequoia

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: macOS Sequoia

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

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

CVE-2025-24236: Csaba Fitzl (@theevilbit) and Nolan Astrein of Kandji

CoreMedia

Available for: macOS Sequoia

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

CoreMedia Playback

Available for: macOS Sequoia

Impact: A malicious app may be able to access private information

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

CVE-2025-30454: pattern-f (@pattern_F_)

CoreServices

Available for: macOS Sequoia

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

Description: This issue was addressed through improved state management.

CVE-2025-31191: Jonathan Bar Or (@yo_yo_yo_jbo) of Microsoft, and an anonymous researcher

CoreText

Available for: macOS Sequoia

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: macOS Sequoia

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

Crash Reporter

Available for: macOS Sequoia

Impact: An app may be able to gain root privileges

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

CVE-2025-24277: Csaba Fitzl (@theevilbit) of Kandji and Gergely Kalman (@gergely_kalman), and an anonymous researcher

curl

Available for: macOS Sequoia

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

Disk Images

Available for: macOS Sequoia

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

Description: A file access issue was addressed with improved input validation.

CVE-2025-24255: an anonymous researcher

DiskArbitration

Available for: macOS Sequoia

Impact: An app may be able to gain root privileges

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

CVE-2025-30456: Gergely Kalman (@gergely_kalman)

DiskArbitration

Available for: macOS Sequoia

Impact: An app may be able to gain root privileges

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24267: an anonymous researcher

Dock

Available for: macOS Sequoia

Impact: A malicious app may be able to access private information

Description: The issue was addressed with improved checks.

CVE-2025-30455: Mickey Jin (@patch1t), and an anonymous researcher

Dock

Available for: macOS Sequoia

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

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

CVE-2025-31187: Rodolphe BRUNETTI (@eisw0lf) of Lupus Nova

dyld

Available for: macOS Sequoia

Impact: Apps that appear to use App Sandbox may be able to launch without restrictions

Description: A library injection issue was addressed with additional restrictions.

CVE-2025-30462: Pietro Francesco Tirenna, Davide Silvetti, Abdel Adim Oisfi of Shielder (shielder.com)

FaceTime

Available for: macOS Sequoia

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

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

CVE-2025-30451: Kirin (@Pwnrin) and luckyu (@uuulucky)

FeedbackLogger

Available for: macOS Sequoia

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

Description: This issue was addressed with improved data protection.

CVE-2025-24281: Rodolphe BRUNETTI (@eisw0lf)

Focus

Available for: macOS Sequoia

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: macOS Sequoia

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

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

CVE-2025-24283: Kirin (@Pwnrin)

Foundation

Available for: macOS Sequoia

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

Description: An access issue was addressed with additional sandbox restrictions on the system pasteboards.

CVE-2025-30461: an anonymous researcher

Foundation

Available for: macOS Sequoia

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

Foundation

Available for: macOS Sequoia

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

Description: An uncontrolled format string issue was addressed with improved input validation.

CVE-2025-24199: Manuel Fernandez (Stackhopper Security)

GPU Drivers

Available for: macOS Sequoia

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

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

CVE-2025-30464: ABC Research s.r.o.

CVE-2025-24273: Wang Yu of Cyberserval

GPU Drivers

Available for: macOS Sequoia

Impact: An app may be able to disclose kernel memory

Description: The issue was addressed with improved bounds checks.

CVE-2025-24256: Anonymous working with Trend Micro Zero Day Initiative, Murray Mike

Handoff

Available for: macOS Sequoia

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

Description: The issue was addressed with improved restriction of data container access.

CVE-2025-30463: mzzzz__

ImageIO

Available for: macOS Sequoia

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

Installer

Available for: macOS Sequoia

Impact: An app may be able to check the existence of an arbitrary path on the file system

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

CVE-2025-24249: YingQi Shi(@Mas0nShi) of DBAppSecurity's WeBin lab and Minghao Lin (@Y1nKoc)

Installer

Available for: macOS Sequoia

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

Description: A logic issue was addressed with improved checks.

CVE-2025-24229: an anonymous researcher

IOGPUFamily

Available for: macOS Sequoia

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

IOMobileFrameBuffer

Available for: macOS Sequoia

Impact: An app may be able to corrupt coprocessor memory

Description: The issue was addressed with improved bounds checks.

CVE-2025-30437: Ye Zhang (@VAR10CK) of Baidu Security

Kerberos Helper

Available for: macOS Sequoia

Impact: A remote attacker may be able to cause unexpected app termination or heap corruption

Description: A memory initialization issue was addressed with improved memory handling.

CVE-2025-24235: Dave G.

Kernel

Available for: macOS Sequoia

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

Description: The issue was addressed with improved checks.

CVE-2025-24204: Koh M. Nakagawa (@tsunek0h) of FFRI Security, Inc.

Kernel

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-2025-24203: Ian Beer of Google Project Zero

Kernel

Available for: macOS Sequoia

Impact: An attacker with user privileges may be able to read kernel memory

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

CVE-2025-24196: Joseph Ravichandran (@0xjprx) of MIT CSAIL

LaunchServices

Available for: macOS Sequoia

Impact: A malicious JAR file may bypass Gatekeeper checks

Description: This issue was addressed with improved handling of executable types.

CVE-2025-24148: Kenneth Chew

libarchive

Available for: macOS Sequoia

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

Libinfo

Available for: macOS Sequoia

Impact: A user may be able to elevate privileges

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

CVE-2025-24195: Paweł Płatek (Trail of Bits)

libnetcore

Available for: macOS Sequoia

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: macOS Sequoia

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: macOS Sequoia

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

Description: This issue was addressed through improved state management.

CVE-2025-24178: an anonymous researcher

libxpc

Available for: macOS Sequoia

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)

libxpc

Available for: macOS Sequoia

Impact: An app may be able to gain elevated privileges

Description: A logic issue was addressed with improved checks.

CVE-2025-24238: an anonymous researcher

Mail

Available for: macOS Sequoia

Impact: "Block All Remote Content" may not apply for all mail previews

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

CVE-2025-24172: an anonymous researcher

manpages

Available for: macOS Sequoia

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

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

CVE-2025-30450: Pwn2car

Maps

Available for: macOS Sequoia

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: macOS Sequoia

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

Notes

Available for: macOS Sequoia

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

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

CVE-2025-24262: LFY@secsys from Fudan University

NSDocument

Available for: macOS Sequoia

Impact: A malicious app may be able to access arbitrary files

Description: This issue was addressed through improved state management.

CVE-2025-24232: an anonymous researcher

OpenSSH

Available for: macOS Sequoia

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

Description: An injection issue was addressed with improved validation.

CVE-2025-24246: 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-2025-24261: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Sequoia

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

Description: A logic issue was addressed with improved checks.

CVE-2025-24164: Mickey Jin (@patch1t)

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-2025-30446: Pedro Tôrres (@t0rr3sp3dr0)

Parental Controls

Available for: macOS Sequoia

Impact: An app may be able to retrieve Safari bookmarks without an entitlement check

Description: This issue was addressed with additional entitlement checks.

CVE-2025-24259: Noah Gregory (wts.dev)

Photos Storage

Available for: macOS Sequoia

Impact: Deleting a conversation in Messages may expose user contact information in system logging

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

CVE-2025-30424: an anonymous researcher

Power Services

Available for: macOS Sequoia

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)

Python

Available for: macOS Sequoia

Impact: A remote attacker may be able to bypass sender policy checks and deliver malicious content via email

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-2023-27043

RPAC

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 validation of environment variables.

CVE-2025-24191: Claudio Bozzato and Francesco Benvenuto of Cisco Talos

Safari

Available for: macOS Sequoia

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

Description: The issue was addressed with improved UI.

CVE-2025-24113: @RenwaX23

Safari

Available for: macOS Sequoia

Impact: Visiting a malicious website may lead to address bar spoofing

Description: The issue was addressed with improved checks.

CVE-2025-30467: @RenwaX23

Safari

Available for: macOS Sequoia

Impact: A website may be able to access sensor information without user consent

Description: The issue was addressed with improved checks.

CVE-2025-31192: Jaydev Ahire

Safari

Available for: macOS Sequoia

Impact: A download's origin may be incorrectly associated

Description: This issue was addressed through improved state management.

CVE-2025-24167: Syarif Muhammad Sajjad

Sandbox

Available for: macOS Sequoia

Impact: An app may be able to access removable volumes without user consent

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24093: Yiğit Can YILMAZ (@yilmazcanyigit)

Sandbox

Available for: macOS Sequoia

Impact: An input validation issue was addressed

Description: The issue was addressed with improved checks.

CVE-2025-30452: an anonymous researcher

Sandbox

Available for: macOS Sequoia

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24181: Arsenii Kostromin (0x3c3e)

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-2025-30458: Mickey Jin (@patch1t)

Security

Available for: macOS Sequoia

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

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-2025-24250: Wojciech Regula of SecuRing (wojciechregula.blog)

Share Sheet

Available for: macOS Sequoia

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: macOS Sequoia

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

Description: A permissions issue was addressed with improved validation.

CVE-2025-30465: an anonymous researcher

Shortcuts

Available for: macOS Sequoia

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

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

CVE-2025-24280: Kirin (@Pwnrin)

Shortcuts

Available for: macOS Sequoia

Impact: A Shortcut may run with admin privileges without authentication

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

CVE-2025-31194: Dolf Hoegaerts

Shortcuts

Available for: macOS Sequoia

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: macOS Sequoia

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

Description: The issue was addressed with improved restriction of data container access.

CVE-2025-31183: Kirin (@Pwnrin), Bohdan Stasiuk (@bohdan_stasiuk)

Siri

Available for: macOS Sequoia

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

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

CVE-2025-30435: K宝 (@Pwnrin) and luckyu (@uuulucky)

Siri

Available for: macOS Sequoia

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

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

CVE-2025-24217: Kirin (@Pwnrin)

Siri

Available for: macOS Sequoia

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)

Siri

Available for: macOS Sequoia

Impact: An app may be able to enumerate devices that have signed into the user's Apple Account

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24248: Minghao Lin (@Y1nKoc) and Tong Liu@Lyutoon_ and 风(binary_fmyy) and F00L

Siri

Available for: macOS Sequoia

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

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

CVE-2025-24205: YingQi Shi(@Mas0nShi) of DBAppSecurity's WeBin lab and Minghao Lin (@Y1nKoc)

Siri

Available for: macOS Sequoia

Impact: An attacker with physical access may be able to use Siri to access sensitive user data

Description: This issue was addressed by restricting options offered on a locked device.

CVE-2025-24198: Richard Hyunho Im (@richeeta) with routezero.security

SMB

Available for: macOS Sequoia

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

Description: The issue was addressed with improved memory handling.

CVE-2025-24269: Alex Radocea of Supernetworks

SMB

Available for: macOS Sequoia

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

Description: A race condition was addressed with improved locking.

CVE-2025-30444: Dave G.

SMB

Available for: macOS Sequoia

Impact: An app may be able to execute arbitrary code with kernel privileges

Description: A buffer overflow issue was addressed with improved memory handling.

CVE-2025-24228: Joseph Ravichandran (@0xjprx) of MIT CSAIL

smbx

Available for: macOS Sequoia

Impact: An attacker in a privileged position may be able to perform a denial-of-service

Description: The issue was addressed with improved memory handling.

CVE-2025-24260: zbleet of QI-ANXIN TianGong Team

Software Update

Available for: macOS Sequoia

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

Description: A library injection issue was addressed with additional restrictions.

CVE-2025-24282: Claudio Bozzato and Francesco Benvenuto of Cisco Talos

Software Update

Available for: macOS Sequoia

Impact: A user may be able to elevate privileges

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

CVE-2025-24254: Arsenii Kostromin (0x3c3e)

Software Update

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-2025-24231: Claudio Bozzato and Francesco Benvenuto of Cisco Talos

StickerKit

Available for: macOS Sequoia

Impact: An app may be able to observe unprotected user data

Description: A privacy issue was addressed by moving sensitive data to a protected location.

CVE-2025-24263: Cristian Dinca of "Tudor Vianu" National High School of Computer Science, Romania

Storage Management

Available for: macOS Sequoia

Impact: An app may be able to enable iCloud storage features without user consent

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24207: YingQi Shi (@Mas0nShi) of DBAppSecurity's WeBin lab, 风沐云烟 (binary_fmyy) and Minghao Lin (@Y1nKoc)

StorageKit

Available for: macOS Sequoia

Impact: An app may be able to gain root privileges

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-30449: Arsenii Kostromin (0x3c3e), and an anonymous researcher

StorageKit

Available for: macOS Sequoia

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

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

CVE-2025-24253: Mickey Jin (@patch1t), Csaba Fitzl (@theevilbit) of Kandji

StorageKit

Available for: macOS Sequoia

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

Description: A race condition was addressed with additional validation.

CVE-2025-24240: Mickey Jin (@patch1t)

StorageKit

Available for: macOS Sequoia

Impact: An app may be able to bypass Privacy preferences

Description: A race condition was addressed with additional validation.

CVE-2025-31188: Mickey Jin (@patch1t)

Summarization Services

Available for: macOS Sequoia

Impact: An app may be able to access information about a user's contacts

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

CVE-2025-24218: Kirin and FlowerCode, Bohdan Stasiuk (@bohdan_stasiuk)

System Settings

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-2025-24278: Zhongquan Li (@Guluisacat)

System Settings

Available for: macOS Sequoia

Impact: An app with root privileges may be able to access private information

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

CVE-2025-24242: Koh M. Nakagawa (@tsunek0h) of FFRI Security, Inc.

SystemMigration

Available for: macOS Sequoia

Impact: A malicious app may be able to create symlinks to protected regions of the disk

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

CVE-2025-30457: Mickey Jin (@patch1t)

Voice Control

Available for: macOS Sequoia

Impact: An app may be able to access contacts

Description: This issue was addressed with improved file handling.

CVE-2025-24279: Mickey Jin (@patch1t)

Web Extensions

Available for: macOS Sequoia

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: macOS Sequoia

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: 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: 285892

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

WebKit Bugzilla: 284055

CVE-2025-24216: Paul Bakker of ParagonERP

WebKit

Available for: macOS Sequoia

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: macOS Sequoia

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

Description: A buffer overflow issue was addressed with improved memory handling.

WebKit Bugzilla: 286462

CVE-2025-24209: Francisco Alonso (@revskills), and an anonymous researcher

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: 285643

CVE-2025-30427: rheza (@ginggilBesel)

WebKit

Available for: macOS Sequoia

Impact: A malicious website may be able to track users in Safari private browsing mode

Description: This issue was addressed through improved state management.

WebKit Bugzilla: 286580

CVE-2025-30425: an anonymous researcher

WindowServer

Available for: macOS Sequoia

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

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

CVE-2025-24247: PixiePoint Security

WindowServer

Available for: macOS Sequoia

Impact: An app may be able to trick a user into copying sensitive data to the pasteboard

Description: A configuration issue was addressed with additional restrictions.

CVE-2025-24241: Andreas Hegenberg (folivora.AI GmbH)

Xsan

Available for: macOS Sequoia

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

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

CVE-2025-24266: an anonymous researcher

Xsan

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-2025-24265: an anonymous researcher

Xsan

Available for: macOS Sequoia

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

Description: A buffer overflow issue was addressed with improved memory handling.

CVE-2025-24157: an anonymous researcher

Additional recognition

Accounts

We would like to acknowledge Bohdan Stasiuk (@bohdan_stasiuk) for their assistance.

AirPlay

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

Entry added April 28, 2025

Analytics

We would like to acknowledge YingQi Shi(@Mas0nShi) of DBAppSecurity's WeBin lab and Minghao Lin (@Y1nKoc) for their assistance.

AppKit

We would like to acknowledge Osintedx for their assistance.

Apple Account

We would like to acknowledge Byron Fecho for their assistance.

AppleMobileFileIntegrity

We would like to acknowledge Jeffrey Hofmann 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 Project Zero for their assistance.

Handoff

We would like to acknowledge Kirin and FlowerCode 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.

Kext Management

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

libnetcore

We would like to acknowledge Wojciech Regula of SecuRing (wojciechregula.blog) for their assistance.

libxpc

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

Login Window

We would like to acknowledge Charles Mangin 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, K宝 and LFY@secsys from Fudan University for their assistance.

Messages

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

MobileAccessoryUpdater

We would like to acknowledge Claudio Bozzato and Francesco Benvenuto of Cisco Talos for their assistance.

Notes

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) of Lakshmi Narain College of Technology Bhopal India for their assistance.

Photos

We would like to acknowledge Bistrit Dahal for their assistance.

Quick Look

We would like to acknowledge Wojciech Regula of SecuRing (wojciechregula.blog), pattern-f (@pattern_F_) for their assistance.

Safari

We would like to acknowledge George Bafaloukas (george.bafaloukas@pingidentity.com) and Shri Hunashikatti (sshpro9@gmail.com) for their assistance.

Safari Downloads

We would like to acknowledge Koh M. Nakagawa (@tsunek0h) of FFRI Security, Inc. for their assistance.

Safari Extensions

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

Sandbox

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

Shortcuts

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

Siri

We would like to acknowledge Lyutoon for their assistance.

SMB

We would like to acknowledge Dave G. for their assistance.

srd_tools

We would like to acknowledge Joshua van Rijswijk, Micheal ogaga, hitarth shah for their assistance.

System Settings

We would like to acknowledge Joshua Jewett (@JoshJewett33) for their assistance.

Translations

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

Weather

We would like to acknowledge Lyutoon for their assistance.

WebKit

We would like to acknowledge Gary Kwong, Junsung Lee, P1umer (@p1umer) and Q1IQ (@q1iqF), 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, 냥냥, 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: April 29, 2025

Helpful? Yes No

Support About the security content of macOS Sequoia 15.4