About the security content of macOS Sequoia 15.3

This document describes the security content of macOS Sequoia 15.3.

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 15.3

Released January 27, 2025

AirPlay

Available for: macOS Sequoia

Impact: An attacker on the local network may be able to cause unexpected system termination or corrupt process memory

Description: An input validation issue was addressed.

CVE-2025-24126: Uri Katz (Oligo Security)

AirPlay

Available for: macOS Sequoia

Impact: A remote attacker may cause an unexpected app termination

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

CVE-2025-24129: Uri Katz (Oligo Security)

AirPlay

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-2025-24131: Uri Katz (Oligo Security)

AirPlay

Available for: macOS Sequoia

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

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

CVE-2025-24177: Uri Katz (Oligo Security)

AirPlay

Available for: macOS Sequoia

Impact: A remote attacker may cause an unexpected application termination or arbitrary code execution

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

CVE-2025-24137: Uri Katz (Oligo Security)

AppKit

Available for: macOS Sequoia

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

Description: The issue was addressed with additional permissions checks.

CVE-2025-24087: Mickey Jin (@patch1t)

AppleGraphicsControl

Available for: macOS Sequoia

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

Description: The issue was addressed with improved checks.

CVE-2025-24112: D4m0n

AppleMobileFileIntegrity

Available for: macOS Sequoia

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

Description: A logic issue was addressed with improved restrictions.

CVE-2025-24100: Kirin (@Pwnrin)

AppleMobileFileIntegrity

Available for: macOS Sequoia

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

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

CVE-2025-24109: Bohdan Stasiuk (@Bohdan_Stasiuk)

AppleMobileFileIntegrity

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-2025-24114: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

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-2025-24121: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

Available for: macOS Sequoia

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

Description: A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions.

CVE-2025-24122: Mickey Jin (@patch1t)

ARKit

Available for: macOS Sequoia

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

Description: The issue was addressed with improved checks.

CVE-2025-24127: Minghao Lin (@Y1nKoc), babywu, and Xingwei Lin of Zhejiang University

Audio

Available for: macOS Sequoia

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

Description: The issue was addressed with improved checks.

CVE-2025-24106: Wang Yu of Cyberserval

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-2025-24160: Google Threat Analysis Group

CVE-2025-24161: Google Threat Analysis Group

CVE-2025-24163: Google Threat Analysis Group

CoreMedia

Available for: macOS Sequoia

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

Description: The issue was addressed with improved checks.

CVE-2025-24123: Desmond working with Trend Micro Zero Day Initiative

CVE-2025-24124: Pwn2car & Rotiple (HyeongSeok Jang) working with Trend Micro Zero Day Initiative

CoreMedia

Available for: macOS Sequoia

Impact: A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2.

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

CVE-2025-24085

CoreRoutine

Available for: macOS Sequoia

Impact: An app may be able to determine a user's current location

Description: The issue was addressed with improved checks.

CVE-2025-24102: Kirin (@Pwnrin)

FaceTime

Available for: macOS Sequoia

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

Description: An information disclosure issue was addressed with improved privacy controls.

CVE-2025-24134: Kirin (@Pwnrin)

iCloud

Available for: macOS Sequoia

Impact: Files downloaded from the internet may not have the quarantine flag applied

Description: This issue was addressed through improved state management.

CVE-2025-24140: Matej Moravec (@MacejkoMoravec)

iCloud Photo Library

Available for: macOS Sequoia

Impact: An app may be able to bypass Privacy preferences

Description: The issue was addressed with improved checks.

CVE-2025-24174: Arsenii Kostromin (0x3c3e), Joshua Jones

ImageIO

Available for: macOS Sequoia

Impact: Processing an image may lead to a denial-of-service

Description: The issue was addressed with improved memory handling.

CVE-2025-24086: DongJun Kim (@smlijun) and JongSeong Kim (@nevul37) in Enki WhiteHat, D4m0n

Kernel

Available for: macOS Sequoia

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

Description: The issue was addressed with improved memory handling.

CVE-2025-24118: Joseph Ravichandran (@0xjprx) of MIT CSAIL

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-2025-24107: an anonymous researcher

Kernel

Available for: macOS Sequoia

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

Description: A validation issue was addressed with improved logic.

CVE-2025-24159: pattern-f (@pattern_F_)

LaunchServices

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-2025-24094: an anonymous researcher

LaunchServices

Available for: macOS Sequoia

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

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

CVE-2025-24115: an anonymous researcher

LaunchServices

Available for: macOS Sequoia

Impact: An app may be able to bypass Privacy preferences

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

CVE-2025-24116: an anonymous researcher

LaunchServices

Available for: macOS Sequoia

Impact: An app may be able to fingerprint the user

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

CVE-2025-24117: Michael (Biscuit) Thomas (@biscuit@social.lol)

Login Window

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-2025-24136: 云散

Messages

Available for: macOS Sequoia

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

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

CVE-2025-24101: Kirin (@Pwnrin)

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-2025-24096: an anonymous researcher

PackageKit

Available for: macOS Sequoia

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

Description: The issue was addressed with improved checks.

CVE-2025-24099: Mickey Jin (@patch1t)

Entry added January 29, 2025

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-2025-24130: Pedro Tôrres (@t0rr3sp3dr0)

Passwords

Available for: macOS Sequoia

Impact: A malicious app may be able to bypass browser extension authentication

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

CVE-2025-24169: Josh Parnham (@joshparnham)

Photos Storage

Available for: macOS Sequoia

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

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

CVE-2025-24146: 神罚(@Pwnrin)

Safari

Available for: macOS Sequoia

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

Description: The issue was addressed by adding additional logic.

CVE-2025-24128: @RenwaX23

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

SceneKit

Available for: macOS Sequoia

Impact: Parsing a file may lead to disclosure of user information

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

CVE-2025-24149: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Security

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-2025-24103: Zhongquan Li (@Guluisacat)

SharedFileList

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.

CVE-2025-24108: an anonymous researcher

sips

Available for: macOS Sequoia

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

Description: The issue was addressed with improved checks.

CVE-2025-24139: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

SMB

Available for: macOS Sequoia

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

Description: The issue was addressed with improved memory handling.

CVE-2025-24151: an anonymous researcher

CVE-2025-24152: an anonymous researcher

SMB

Available for: macOS Sequoia

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

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

CVE-2025-24153: an anonymous researcher

Spotlight

Available for: macOS Sequoia

Impact: A malicious application may be able to leak sensitive user information

Description: This issue was addressed through improved state management.

CVE-2025-24138: Rodolphe BRUNETTI (@eisw0lf) of Lupus Nova

StorageKit

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-2025-24107: an anonymous researcher

StorageKit

Available for: macOS Sequoia

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

Description: A permissions issue was addressed with improved validation.

CVE-2025-24176: Yann GASCUEL of Alter Solutions

System Extensions

Available for: macOS Sequoia

Impact: An app may be able to gain elevated privileges

Description: This issue was addressed with improved message validation.

CVE-2025-24135: Arsenii Kostromin (0x3c3e)

Time Zone

Available for: macOS Sequoia

Impact: An app may be able to view a contact's phone number in system logs

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

CVE-2025-24145: Kirin (@Pwnrin)

TV App

Available for: macOS Sequoia

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

Description: This issue was addressed with improved data protection.

CVE-2025-24092: Adam M.

WebContentFilter

Available for: macOS Sequoia

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

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

CVE-2025-24154: an anonymous researcher

WebKit

Available for: macOS Sequoia

Impact: A maliciously crafted webpage may be able to fingerprint the user

Description: The issue was addressed with improved access restrictions to the file system.

WebKit Bugzilla: 283117

CVE-2025-24143: an anonymous researcher

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: 283889

CVE-2025-24158: Q1IQ (@q1iqF) of NUS CuriOSity and P1umer (@p1umer) of Imperial Global Singapore.

WebKit

Available for: macOS Sequoia

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

Description: This issue was addressed through improved state management.

WebKit Bugzilla: 284159

CVE-2025-24162: linjy of HKUS3Lab and chluo of WHUSecLab

WebKit Web Inspector

Available for: macOS Sequoia

Impact: Copying a URL from Web Inspector may lead to command injection

Description: A privacy issue was addressed with improved handling of files.

WebKit Bugzilla: 283718

CVE-2025-24150: Johan Carlsson (joaxcar)

WindowServer

Available for: macOS Sequoia

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

Description: This issue was addressed by improved management of object lifetimes.

CVE-2025-24120: PixiePoint Security

Xsan

Available for: macOS Sequoia

Impact: An app may be able to elevate privileges

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

CVE-2025-24156: an anonymous researcher

Additional recognition

Audio

We would like to acknowledge Google Threat Analysis Group for their assistance.

CoreAudio

We would like to acknowledge Google Threat Analysis Group for their assistance.

CoreMedia Playback

We would like to acknowledge Song Hyun Bae (@bshyuunn) and Lee Dong Ha (Who4ml) for their assistance.

DesktopServices

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

Files

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

Passwords

We would like to acknowledge Talal Haj Bakry and Tommy Mysk of Mysk Inc. @mysk_co for their assistance.

sips

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

Static Linker

We would like to acknowledge Holger Fuhrmannek for their assistance.

VoiceOver

We would like to acknowledge Bistrit Dahal, Dalibor Milanovic for their assistance.

Published Date: January 29, 2025