About the security content of macOS Sequoia 15.1

This document describes the security content of macOS Sequoia 15.1.

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 15.1

Released October 28, 2024

Apache

Impact: Multiple issues existed in Apache

Description: This is a vulnerability in open source code and Apple Software 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-2024-39573

CVE-2024-38477

CVE-2024-38476

App Support

Available for: macOS Sequoia

Impact: A malicious app may be able to run arbitrary shortcuts without user consent

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

CVE-2024-44255: an anonymous researcher

AppleAVD

Available for: macOS Sequoia

Impact: Parsing a maliciously crafted video file may lead to unexpected system termination

Description: The issue was addressed with improved bounds checks.

CVE-2024-44232: Ivan Fratric of Google Project Zero

CVE-2024-44233: Ivan Fratric of Google Project Zero

CVE-2024-44234: Ivan Fratric of Google Project Zero

Entry added November 1, 2024

AppleMobileFileIntegrity

Available for: macOS Sequoia

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

Description: A logic issue was addressed with improved validation.

CVE-2024-44270: 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-2024-44280: Mickey Jin (@patch1t)

Assets

Available for: macOS Sequoia

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

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

CVE-2024-44260: Mickey Jin (@patch1t)

Calendar

Available for: macOS Sequoia

Impact: An attacker with access to calendar data could also read reminders

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

CVE-2024-54535: K宝(@Pwnrin)

Entry added January 15, 2025

Contacts

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-2024-44298: Kirin (@Pwnrin) and 7feilee

CoreMedia Playback

Available for: macOS Sequoia

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

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

CVE-2024-44273: pattern-f (@pattern_F_), Hikerell of Loadshine Lab

CoreServicesUIAgent

Available for: macOS Sequoia

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

Description: This issue was addressed with additional entitlement checks.

CVE-2024-44295: an anonymous researcher

CoreText

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 checks.

CVE-2024-44240: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CVE-2024-44302: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

Dock

Available for: macOS Sequoia

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

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

CVE-2024-54554: Mickey Jin (@patch1t)

Entry added August 28, 2025

CUPS

Available for: macOS Sequoia

Impact: An attacker in a privileged network position may be able to leak sensitive user information

Description: An issue existed in the parsing of URLs. This issue was addressed with improved input validation.

CVE-2024-44213: Alexandre Bedard

Find My

Available for: macOS Sequoia

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

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

CVE-2024-44289: Kirin (@Pwnrin)

Foundation

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 input validation.

CVE-2024-44282: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

Game Controllers

Available for: macOS Sequoia

Impact: An attacker with physical access can input Game Controller events to apps running on a locked device

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

CVE-2024-44265: Ronny Stiftel

GPU Drivers

Available for: macOS Sequoia

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

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

CVE-2024-40854: Wang Yu of Cyberserval

Entry added January 15, 2025

ImageIO

Available for: macOS Sequoia

Impact: Processing an image may result in disclosure of process memory

Description: This issue was addressed with improved checks.

CVE-2024-44215: Junsung Lee working with Trend Micro Zero Day Initiative

ImageIO

Available for: macOS Sequoia

Impact: Processing a maliciously crafted message may lead to a denial-of-service

Description: The issue was addressed with improved bounds checks.

CVE-2024-44297: Jex Amro

Installer

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-2024-44216: Zhongquan Li (@Guluisacat)

Installer

Available for: macOS Sequoia

Impact: A malicious application may be able to modify protected parts of the file system

Description: The issue was addressed with improved checks.

CVE-2024-44287: Mickey Jin (@patch1t)

IOGPUFamily

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-2024-44197: Wang Yu of Cyberserval

Entry updated August 28, 2025

IOMobileFrameBuffer

Available for: macOS Sequoia

Impact: An attacker may be able to cause unexpected system termination or arbitrary code execution in DCP firmware

Description: The issue was addressed with improved bounds checks.

CVE-2024-44299: Ye Zhang (@VAR10CK) of Baidu Security

CVE-2024-44241: Ye Zhang (@VAR10CK) of Baidu Security

CVE-2024-44242: Ye Zhang (@VAR10CK) of Baidu Security

Entry added December 11, 2024

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-2024-44238: Ye Zhang (@VAR10CK) of Baidu Security

Entry added January 16, 2026

IOSurface

Available for: macOS Sequoia

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

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

CVE-2024-44285: an anonymous researcher

Kernel

Available for: macOS Sequoia

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

Description: An information disclosure issue was addressed with improved private data redaction for log entries.

CVE-2024-44239: Mateusz Krzywicki (@krzywix)

LaunchServices

Available for: macOS Sequoia

Impact: An attacker with physical access can input keyboard events to apps running on a locked device

Description: This issue was addressed through improved state management.

CVE-2024-44286: Garrett Moon of Excited Pixel LLC

Entry added January 15, 2025

LaunchServices

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-2024-40849: Arsenii Kostromin (0x3c3e)

Entry added December 11, 2024

libarchive

Available for: macOS Sequoia

Impact: Processing a malicious crafted file may lead to a denial-of-service

Description: The issue was addressed with improved memory handling.

CVE-2024-44201: Ben Roeder

Entry added December 11, 2024

Login Window

Available for: macOS Sequoia

Impact: A person with physical access to a Mac may be able to bypass Login Window during a software update

Description: This issue was addressed through improved state management.

CVE-2024-44231: Toomas Römer

Login Window

Available for: macOS Sequoia

Impact: An attacker with physical access to a Mac may be able to view protected content from the Login Window

Description: This issue was addressed through improved state management.

CVE-2024-44223: Jaime Bertran

Maps

Available for: macOS Sequoia

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

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

CVE-2024-44222: Kirin (@Pwnrin)

Messages

Available for: macOS Sequoia

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

Description: The issue was addressed with improved input sanitization.

CVE-2024-44256: Mickey Jin (@patch1t)

NetAuth

Available for: macOS Sequoia

Impact: A malicious application may be able to leak a user's credentials

Description: This issue was addressed with additional entitlement checks.

CVE-2024-54471: Noah Gregory (wts.dev)

Entry added December 11, 2024

Notification Center

Available for: macOS Sequoia

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

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

CVE-2024-44292: Kirin (@Pwnrin)

Notification Center

Available for: macOS Sequoia

Impact: A user may be able to view sensitive user information

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

CVE-2024-44293: Kirin (@Pwnrin) and 7feilee

PackageKit

Available for: macOS Sequoia

Impact: A malicious application may be able to modify protected parts of the file system

Description: The issue was addressed with improved checks.

CVE-2024-44247: Un3xploitable of CW Research Inc

CVE-2024-44267: Bohdan Stasiuk (@Bohdan_Stasiuk), Un3xploitable of CW Research Inc, Pedro Tôrres (@t0rr3sp3dr0)

CVE-2024-44301: Bohdan Stasiuk (@Bohdan_Stasiuk), Un3xploitable of CW Research Inc, Pedro Tôrres (@t0rr3sp3dr0)

CVE-2024-44275: Arsenii Kostromin (0x3c3e)

CVE-2024-44303: Pedro Tôrres (@t0rr3sp3dr0)

Entry updated December 11, 2024

PackageKit

Available for: macOS Sequoia

Impact: An app may be able to bypass Privacy preferences

Description: A path deletion vulnerability was addressed by preventing vulnerable code from running with privileges.

CVE-2024-44156: Arsenii Kostromin (0x3c3e)

CVE-2024-44159: 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-2024-44253: Mickey Jin (@patch1t), Csaba Fitzl (@theevilbit) of Kandji

PackageKit

Available for: macOS Sequoia

Impact: An attacker with root privileges may be able to delete protected system files

Description: A path deletion vulnerability was addressed by preventing vulnerable code from running with privileges.

CVE-2024-44294: Mickey Jin (@patch1t)

PackageKit

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-2024-44196: Csaba Fitzl (@theevilbit) of Kandji

Photos

Available for: macOS Sequoia

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2024-40858: Csaba Fitzl (@theevilbit) of Kandji

Pro Res

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-2024-44277: an anonymous researcher and Yinyi Wu(@_3ndy1) from Dawn Security Lab of JD.com, Inc.

Quick Look

Available for: macOS Sequoia

Impact: An app may be able to read arbitrary files

Description: A logic issue was addressed with improved validation.

CVE-2024-44195: an anonymous researcher

Safari Downloads

Available for: macOS Sequoia

Impact: An attacker may be able to misuse a trust relationship to download malicious content

Description: This issue was addressed through improved state management.

CVE-2024-44259: Narendra Bhati, Manager of Cyber Security at Suma Soft Pvt. Ltd, Pune (India)

Safari Private Browsing

Available for: macOS Sequoia

Impact: Private browsing may leak some browsing history

Description: An information leakage was addressed with additional validation.

CVE-2024-44229: Lucas Di Tomase

Sandbox

Available for: macOS Sequoia

Impact: A malicious application with root privileges may be able to access private information

Description: A permissions issue was addressed with additional restrictions.

CVE-2024-44219: Ryan Dowd (@_rdowd)

Entry added December 11, 2024

Sandbox

Available for: macOS Sequoia

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

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

CVE-2024-44211: Gergely Kalman (@gergely_kalman) and Csaba Fitzl (@theevilbit)

SceneKit

Available for: macOS Sequoia

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

Description: This issue was addressed with improved checks.

CVE-2024-44218: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Screen Sharing Server

Available for: macOS Sequoia

Impact: A user with screen sharing access may be able to view another user's screen

Description: This issue was addressed through improved state management.

CVE-2024-44248: Halle Winkler, Politepix (theoffcuts.org)

Entry added December 11, 2024

Security

Available for: macOS Sequoia

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

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

CVE-2024-54538: Bing Shi, Wenchao Li and Xiaolong Bai of Alibaba Group, and Luyi Xing of Indiana University Bloomington

Entry added December 19, 2024

Shortcuts

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-2024-44254: Kirin (@Pwnrin)

Shortcuts

Available for: macOS Sequoia

Impact: A malicious app may use shortcuts to access restricted files

Description: A logic issue was addressed with improved checks.

CVE-2024-44269: Kirin (@Pwnrin) and an anonymous researcher

Entry updated December 11, 2024

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-2024-44236: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CVE-2024-44237: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

sips

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 input validation.

CVE-2024-44279: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CVE-2024-44281: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

sips

Available for: macOS Sequoia

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

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

CVE-2024-44283: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

sips

Available for: macOS Sequoia

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

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

CVE-2024-44284: Junsung Lee, dw0r! working with Trend Micro Zero Day Initiative

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-2024-44194: Rodolphe Brunetti (@eisw0lf)

Siri

Available for: macOS Sequoia

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

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

CVE-2024-44200: Cristian Dinca (icmd.tech)

Entry added December 11, 2024

Siri

Available for: macOS Sequoia

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

Description: An information disclosure issue was addressed with improved private data redaction for log entries.

CVE-2024-44278: Kirin (@Pwnrin)

StorageKit

Available for: macOS Sequoia

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

Description: This issue was addressed with improved permissions checking.

CVE-2024-44210: Mickey Jin (@patch1t), Csaba Fitzl (@theevilbit) of Kandji

Entry added January 16, 2026

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-2024-44264: Mickey Jin (@patch1t)

Weather

Available for: macOS Sequoia

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

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

CVE-2024-44290: Kirin (@Pwnrin)

Entry added December 11, 2024

WebKit

Available for: macOS Sequoia

Impact: Processing maliciously crafted web content may prevent Content Security Policy from being enforced

Description: The issue was addressed with improved checks.

WebKit Bugzilla: 278765

CVE-2024-44296: Narendra Bhati, Manager of Cyber Security at Suma Soft Pvt. Ltd, Pune (India)

WebKit

Available for: macOS Sequoia

Impact: Cookies belonging to one origin may be sent to another origin

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

WebKit Bugzilla: 279226

CVE-2024-44212: Wojciech Regula of SecuRing (wojciechregula.blog)

Entry added December 11, 2024

WebKit

Available for: macOS Sequoia

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

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

WebKit Bugzilla: 279780

CVE-2024-44244: an anonymous researcher, Q1IQ (@q1iqF) and P1umer (@p1umer)

WindowServer

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-2024-44257: Bohdan Stasiuk (@Bohdan_Stasiuk)

XPC

Available for: macOS Sequoia

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2024-44250: Mickey Jin (@patch1t)

Entry added January 15, 2025

Additional recognition

Airport

We would like to acknowledge Bohdan Stasiuk (@Bohdan_Stasiuk), K宝(@Pwnrin) for their assistance.

Calculator

We would like to acknowledge Kenneth Chew for their assistance.

Calendar

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

ImageIO

We would like to acknowledge Amir Bazine and Karsten König of CrowdStrike Counter Adversary Operations, an anonymous researcher for their assistance.

Messages

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

NetworkExtension

We would like to acknowledge Patrick Wardle of DoubleYou & the Objective-See Foundation for their assistance.

Notification Center

We would like to acknowledge Kirin (@Pwnrin) and LFYSec for their assistance.

Open vSwitch

We would like to acknowledge David Coomber for their assistance.

Entry added January 15, 2025

Photos

We would like to acknowledge James Robertson for their assistance.

Safari Private Browsing

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

Entry updated December 11, 2024

Safari Tabs

We would like to acknowledge Jaydev Ahire for their assistance.

Siri

We would like to acknowledge Bistrit Dahal for their assistance.

Published Date: January 16, 2026