

About the security content of macOS Sequoia 15.7.4

This document describes the security content of macOS Sequoia 15.7.4.

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 15.7.4

Released February 11, 2026

AppleMobileFileIntegrity

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-2026-20624: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

Available for: macOS Sequoia

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

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

CVE-2026-20625: Mickey Jin (@patch1t), Ryan Dowd (@_rdowd)

Compression

Available for: macOS Sequoia

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

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

CVE-2025-43403: Mickey Jin (@patch1t)

CoreAudio

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-2026-20611: Anonymous working with Trend Micro Zero Day Initiative

CoreMedia

Available for: macOS Sequoia

Impact: Processing a maliciously crafted file may lead to a denial-of-service or potentially disclose memory contents

Description: The issue was addressed with improved memory handling.

CVE-2026-20609: Yiğit Can YILMAZ (@yilmazcanyigit)

GPU Drivers

Available for: macOS Sequoia

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

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

CVE-2026-20620: Murray Mike

ImageIO

Available for: macOS Sequoia

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

Description: The issue was addressed with improved memory handling.

CVE-2026-20634: George Karchemsky (@gkarchemsky) working with Trend Micro Zero Day Initiative

ImageIO

Available for: macOS Sequoia

Impact: Processing a maliciously crafted image may lead to disclosure of user information

Description: The issue was addressed with improved bounds checks.

CVE-2026-20675: George Karchemsky (@gkarchemsky) working with Trend Micro Zero Day Initiative

Kernel

Available for: macOS Sequoia

Impact: An attacker in a privileged network position may be able to intercept network traffic

Description: A logic issue was addressed with improved checks.

CVE-2026-20671: Xin'an Zhou, Juefei Pu, Zhutian Liu, Zhiyun Qian, Zhaowei Tan, Srikanth V. Krishnamurthy, Mathy Vanhoef

Kernel

Available for: macOS Sequoia

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

Description: This issue was addressed with improved checks.

CVE-2026-20626: Keisuke Hosoda

libexpat

Available for: macOS Sequoia

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

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-2025-59375

libnetcore

Available for: macOS Sequoia

Impact: An attacker in a privileged network position may be able to intercept network traffic

Description: A logic issue was addressed with improved checks.

CVE-2026-20671: Xin'an Zhou, Juefei Pu, Zhutian Liu, Zhiyun Qian, Zhaowei Tan, Srikanth V. Krishnamurthy, Mathy Vanhoef

libxpc

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-2026-20667: an anonymous researcher

Mail

Available for: macOS Sequoia

Impact: Turning off "Load remote content in messages" may not apply to all mail previews

Description: A logic issue was addressed with improved checks.

CVE-2026-20673: an anonymous researcher

MigrationKit

Available for: macOS Sequoia

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

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

CVE-2026-20694: Rodolphe Brunetti (@eisw0lf) of Lupus Nova

Entry added March 24, 2026

Multi-Touch

Available for: macOS Sequoia

Impact: A malicious HID device may cause an unexpected process crash

Description: The issue was addressed with improved bounds checks.

CVE-2025-43533: Google Threat Analysis Group

CVE-2025-46300: Google Threat Analysis Group

CVE-2025-46301: Google Threat Analysis Group

CVE-2025-46302: Google Threat Analysis Group

CVE-2025-46303: Google Threat Analysis Group

CVE-2025-46304: Google Threat Analysis Group

CVE-2025-46305: Google Threat Analysis Group

PackageKit

Available for: macOS Sequoia

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

Description: This issue was addressed through improved state management.

CVE-2025-46310: Mickey Jin (@patch1t)

Remote Management

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-2026-20614: Gergely Kalman (@gergely_kalman)

Sandbox

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-2026-20628: Noah Gregory (wts.dev)

Security

Available for: macOS Sequoia

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

Description: A logic issue was addressed with improved checks.

CVE-2025-46290: Bing Shi, Wenchao Li and Xiaolong Bai of Alibaba Group, and Luyi Xing of Indiana University Bloomington

Shortcuts

Available for: macOS Sequoia

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

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

CVE-2026-20653: Enis Maholli (enismaholli.com)

Shortcuts

Available for: macOS Sequoia

Impact: An app may be able to capture a user's screen

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

CVE-2026-20622: Csaba Fitzl (@theevilbit) of Iru

Entry added March 24, 2026

Siri

Available for: macOS Sequoia

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

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

CVE-2026-20662: Vivek Dhar, ASI (RM) in Border Security Force, FTR HQ BSF Kashmir

Spotlight

Available for: macOS Sequoia

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

Description: The issue was addressed with additional restrictions on the observability of app states.

CVE-2026-20680: an anonymous researcher

Spotlight

Available for: macOS Sequoia

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

Description: A privacy issue was addressed with improved checks.

CVE-2026-20612: Mickey Jin (@patch1t)

StoreKit

Available for: macOS Sequoia

Impact: An app may be able to identify what other apps a user has installed

Description: A privacy issue was addressed with improved checks.

CVE-2026-20641: Gongyu Ma (@Mezone0)

System Settings

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-2026-20619: Asaf Cohen

UIKit

Available for: macOS Sequoia

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

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

CVE-2026-20606: LeminLimez

Voice Control

Available for: macOS Sequoia

Impact: An app may be able to crash a system process

Description: The issue was addressed with improved memory handling.

CVE-2026-20605: @cloudlldb of @pixiepointsec

Wi-Fi

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-2026-20621: Wang Yu of Cyberserval

WindowServer

Available for: macOS Sequoia

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

Description: The issue was addressed with improved memory handling.

CVE-2025-43402: @cloudlldb of @pixiepointsec

WindowServer

Available for: macOS Sequoia

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

Description: The issue was addressed with improved handling of caches.

CVE-2026-20602: @cloudlldb of @pixiepointsec

Additional recognition

CoreServices

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

Kernel

We would like to acknowledge Xinru Chi of Pangu Lab for their assistance.

libpthread

We would like to acknowledge Fabiano Anemone for their assistance.

WindowServer

We would like to acknowledge @cloudlldb of @pixiepointsec 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: March 24, 2026

Helpful?

Yes

No

 > Support > About the security content of macOS Sequoia 15.7.4

Copyright © 2026 Apple Inc. All rights reserved. [Privacy Policy](#) | [Terms of Use](#) | [Sales and Refunds](#) | [Site Map](#)

United States