About the security content of macOS Sonoma 14.8.4

This document describes the security content of macOS Sonoma 14.8.4.

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 Sonoma 14.8.4

Released February 11, 2026

AppleEvents

Available for: macOS Sonoma

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

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

CVE-2026-20670: Noah Gregory (wts.dev)

Entry added March 24, 2026

AppleMobileFileIntegrity

Available for: macOS Sonoma

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 Sonoma

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)

CFNetwork

Available for: macOS Sonoma

Impact: A remote user may be able to write arbitrary files

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

CVE-2026-20660: Amy (amys.website)

Compression

Available for: macOS Sonoma

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 Sonoma

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 Sonoma

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)

CoreServices

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

Description: A race condition was addressed with improved state handling.

CVE-2026-20617: Golden Helm Securities, Gergely Kalman (@gergely_kalman), Csaba Fitzl (@theevilbit) of Iru

Entry updated March 24, 2026

CoreServices

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

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

CVE-2026-20615: Csaba Fitzl (@theevilbit) of Iru and Gergely Kalman (@gergely_kalman)

CoreServices

Available for: macOS Sonoma

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

Description: A logic issue was addressed with improved validation.

CVE-2025-46283: an anonymous researcher

CoreServices

Available for: macOS Sonoma

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-2026-20627: an anonymous researcher

File Bookmark

Available for: macOS Sonoma

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

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

CVE-2025-43417: Ron Elemans

GPU Drivers

Available for: macOS Sonoma

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 Sonoma

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-2025-43338: 이동하 (Lee Dong Ha) of SSA Lab

ImageIO

Available for: macOS Sonoma

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 Sonoma

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 Sonoma

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

libexpat

Available for: macOS Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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

Messages

Available for: macOS Sonoma

Impact: A shortcut may be able to bypass sandbox restrictions

Description: A race condition was addressed with improved handling of symbolic links.

CVE-2026-20677: Ron Masas of BreakPoint.SH

Messages

Available for: macOS Sonoma

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

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

CVE-2026-20651: Chunyu Song of NorthSea

Entry added March 24, 2026

MigrationKit

Available for: macOS Sonoma

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

Model I/O

Available for: macOS Sonoma

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

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

CVE-2026-20616: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Multi-Touch

Available for: macOS Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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)

Spotlight

Available for: macOS Sonoma

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 Sonoma

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 Sonoma

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)

UIKit

Available for: macOS Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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 Golden Helm Securities, YingQi Shi (@Mas0nShi) of DBAppSecurity's WeBin lab, Csaba Fitzl (@theevilbit) of Iru and Gergely Kalman (@gergely_kalman) 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.

Published Date: March 24, 2026