About the security content of macOS Sonoma 14.8.5

This document describes the security content of macOS Sonoma 14.8.5.

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 14.8.5

Released March 24, 2026

802.1X

Available for: macOS Sonoma

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

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

CVE-2026-28865: Héloïse Gollier and Mathy Vanhoef (KU Leuven)

apache

Available for: macOS Sonoma

Impact: Multiple issues in Apache

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-2025-55753

CVE-2025-58098

CVE-2025-59775

CVE-2025-65082

CVE-2025-66200

AppleKeyStore

Available for: macOS Sonoma

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

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

CVE-2026-20637: Johnny Franks (zeroxjf), an anonymous researcher

AppleMobileFileIntegrity

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-2026-28824: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

Available for: macOS Sonoma

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

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

CVE-2026-20699: Mickey Jin (@patch1t)

Archive Utility

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-2026-20633: Mickey Jin (@patch1t)

Audio

Available for: macOS Sonoma

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

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

CVE-2026-28879: Justin Cohen of Google

Audio

Available for: macOS Sonoma

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

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

CVE-2026-28822: Jex Amro

Calling Framework

Available for: macOS Sonoma

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-2026-28894: an anonymous researcher

Clipboard

Available for: macOS Sonoma

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

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

CVE-2026-28866: Cristian Dinca (icmd.tech)

configd

Available for: macOS Sonoma

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

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

CVE-2026-20639: @cloudlldb of @pixiepointsec

CoreMedia

Available for: macOS Sonoma

Impact: Processing an audio stream in a maliciously crafted media file may terminate the process

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

CVE-2026-20690: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreServices

Available for: macOS Sonoma

Impact: An app may be able to gain elevated privileges

Description: A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement.

CVE-2026-28821: YingQi Shi (@Mas0nShi) of DBAppSecurity's WeBin lab

CoreServices

Available for: macOS Sonoma

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

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

CVE-2026-28838: an anonymous researcher

CoreUtils

Available for: macOS Sonoma

Impact: A user in a privileged network position may be able to cause a denial-of-service

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

CVE-2026-28886: Etienne Charron (Renault) and Victoria Martini (Renault)

Crash Reporter

Available for: macOS Sonoma

Impact: An app may be able to enumerate a user's installed apps

Description: A privacy issue was addressed by removing sensitive data.

CVE-2026-28878: Zhongcheng Li from IES Red Team

CUPS

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-2026-28888: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

curl

Available for: macOS Sonoma

Impact: An issue existed in curl which may result in unintentionally sending sensitive information via an incorrect connection

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-2025-14524

DeviceLink

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-2026-28876: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

Diagnostics

Available for: macOS Sonoma

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

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

CVE-2026-28892: 风沐云烟 (@binary_fmyy) and Minghao Lin (@Y1nKoc)

File System

Available for: macOS Sonoma

Impact: An app may be able to disclose kernel memory

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

CVE-2026-28832: DARKNAVY (@DarkNavyOrg)

Focus

Available for: macOS Sonoma

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

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

CVE-2026-20668: Kirin (@Pwnrin)

GPU Drivers

Available for: macOS Sonoma

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

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

CVE-2026-28834: an anonymous researcher

iCloud

Available for: macOS Sonoma

Impact: An app may be able to enumerate a user's installed apps

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-28880: Zhongcheng Li from IES Red Team

ImageIO

Available for: macOS Sonoma

Impact: Processing a maliciously crafted file may lead to 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-2025-64505

Kernel

Available for: macOS Sonoma

Impact: An app may be able to disclose kernel memory

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

CVE-2026-28868: 이동하 (Lee Dong Ha of BoB 0xB6)

Kernel

Available for: macOS Sonoma

Impact: An app may be able to determine kernel memory layout

Description: An information disclosure issue was addressed with improved memory management.

CVE-2026-20695: 이동하 (Lee Dong Ha of BoB 0xB6) working with TrendAI Zero Day Initiative, hari shanmugam

Kernel

Available for: macOS Sonoma

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-28829: Sreejith Krishnan R

libxpc

Available for: macOS Sonoma

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-20607: an anonymous researcher

Mail

Available for: macOS Sonoma

Impact: "Hide IP Address" and "Block All Remote Content" may not apply to all mail content

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

CVE-2026-20692: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

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

NetAuth

Available for: macOS Sonoma

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

Description: A race condition was addressed with additional validation.

CVE-2026-28891: an anonymous researcher

NetAuth

Available for: macOS Sonoma

Impact: An app may be able to connect to a network share without user consent

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

CVE-2026-20701: Matej Moravec (@MacejkoMoravec)

NetAuth

Available for: macOS Sonoma

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

Description: The issue was addressed with improved checks.

CVE-2026-28839: Mickey Jin (@patch1t)

NetFSFramework

Available for: macOS Sonoma

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

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

CVE-2026-28827: Csaba Fitzl (@theevilbit) of Iru, an anonymous researcher

Notes

Available for: macOS Sonoma

Impact: An app may be able to delete files for which it does not have permission

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

CVE-2026-28816: Dawuge of Shuffle Team and Hunan University

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-2026-20693: Mickey Jin (@patch1t)

Phone

Available for: macOS Sonoma

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

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

CVE-2026-28862: Kun Peeks (@SwayZGl1tZyyy)

Printing

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-2026-28831: an anonymous researcher

Printing

Available for: macOS Sonoma

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

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

CVE-2026-28817: Gyujeong Jin (@G1uN4sh) at Team.0xb6

Printing

Available for: macOS Sonoma

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

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

CVE-2026-20688: wdszzml and Atuin Automated Vulnerability Discovery Engine

Security

Available for: macOS Sonoma

Impact: A local attacker may gain access to user's Keychain items

Description: This issue was addressed with improved permissions checking.

CVE-2026-28864: Alex Radocea

SMB

Available for: macOS Sonoma

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

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

CVE-2026-28835: Christian Kohlschütter

SMB

Available for: macOS Sonoma

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

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

CVE-2026-28825: Sreejith Krishnan R

Spotlight

Available for: macOS Sonoma

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

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

CVE-2026-20699: Mickey Jin (@patch1t)

Spotlight

Available for: macOS Sonoma

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

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

CVE-2026-28818: @pixiepointsec

Spotlight

Available for: macOS Sonoma

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-20697: @pixiepointsec

TCC

Available for: macOS Sonoma

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

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

CVE-2026-28828: Mickey Jin (@patch1t)

Vision

Available for: macOS Sonoma

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

Description: The issue was addressed with improved memory handling.

CVE-2026-20657: Andrew Becker

WebDAV

Available for: macOS Sonoma

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-28829: Sreejith Krishnan R

Additional recognition

Admin Framework

We would like to acknowledge Sota Toyokura for their assistance.

CoreServices

We would like to acknowledge Fein, Iccccc & Ziiiro for their assistance.

CUPS

We would like to acknowledge Csaba Fitzl (@theevilbit) of Iru for their assistance.

Kernel

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

Notes

We would like to acknowledge Dawuge of Shuffle Team and Hunan University for their assistance.

ppp

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

Published Date: March 24, 2026