

About the security content of macOS Sonoma 14.7.3

This document describes the security content of macOS Sonoma 14.7.3.

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 Sonoma 14.7.3

Released January 27, 2025

AirPlay

Available for: macOS Sonoma

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)

AppleGraphicsControl

Available for: macOS Sonoma

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 Sonoma

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 Sonoma

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 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-2025-24114: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

Available for: macOS Sonoma

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 Sonoma

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 Sonoma

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

ASP TCP

Available for: macOS Sonoma

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

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

CVE-2024-54509: CertiK SkyFall Team

Audio

Available for: macOS Sonoma

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

Contacts

Available for: macOS Sonoma

Impact: An app may be able to access contacts

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

CVE-2024-44172: Kirin (@Pwnrin)

CoreAudio

Available for: macOS Sonoma

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

Description: The issue was addressed with improved checks.

CVE-2025-24161: Google Threat Analysis Group

CVE-2025-24160: Google Threat Analysis Group

CVE-2025-24163: Google Threat Analysis Group

CoreMedia

Available for: macOS Sonoma

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

CoreRoutine

Available for: macOS Sonoma

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)

iCloud Photo Library

Available for: macOS Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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 Sonoma

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

Login Window

Available for: macOS Sonoma

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

PackageKit

Available for: macOS Sonoma

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 Sonoma

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 Tôrrres (@t0rr3sp3dr0)

Photos Storage

Available for: macOS Sonoma

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: 神罰(@Pwnrin)

QuartzCore

Available for: macOS Sonoma

Impact: Processing web content may lead to a denial-of-service

Description: The issue was addressed with improved checks.

CVE-2024-54497: Anonymous working with Trend Micro Zero Day Initiative

Sandbox

Available for: macOS Sonoma

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24093: Yiğit Can YILMAZ (@yilmazcanyigit)

SceneKit

Available for: macOS Sonoma

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 Sonoma

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)

sips

Available for: macOS Sonoma

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 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-2025-24151: an anonymous researcher

Spotlight

Available for: macOS Sonoma

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 Sonoma

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

Description: A configuration issue was addressed with additional restrictions.

CVE-2024-44243: Jonathan Bar Or (@yo_yo_yo_jbo) of Microsoft, Mickey Jin (@patch1t)

StorageKit

Available for: macOS Sonoma

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

TV App

Available for: macOS Sonoma

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 Sonoma

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

WindowServer

Available for: macOS Sonoma

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 Sonoma

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

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.

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: January 29, 2025

Helpful? ☐ Yes ☐ No

Support About the security content of macOS Sonoma 14.7.3