About the security content of macOS Sonoma 14.4

This document describes the security content of macOS Sonoma 14.4.

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 14.4

Released March 7, 2024

Accessibility

Available for: macOS Sonoma

Impact: A malicious app may be able to observe user data in log entries related to accessibility notifications

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

CVE-2024-23291

Admin Framework

Available for: macOS Sonoma

Impact: An app may be able to elevate privileges

Description: A logic issue was addressed with improved checks.

CVE-2024-23276: Kirin (@Pwnrin)

Airport

Available for: macOS Sonoma

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

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

CVE-2024-23227: Brian McNulty

AppKit

Available for: macOS Sonoma

Impact: An unprivileged app may be able to log keystrokes in other apps including those using secure input mode

Description: A logic issue was addressed with improved restrictions.

CVE-2024-27886: Stephan Casas and an anonymous researcher

Entry added July 29, 2024

AppleMobileFileIntegrity

Available for: macOS Sonoma

Impact: Entitlements and privacy permissions granted to this app may be used by a malicious app

Description: This issue was addressed with improved checks.

CVE-2024-23233: 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-2024-23269: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

Available for: macOS Sonoma

Impact: An app may be able to elevate privileges

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

CVE-2024-23288: Wojciech Regula of SecuRing (wojciechregula.blog) and Kirin (@Pwnrin)

Bluetooth

Available for: macOS Sonoma

Impact: An attacker in a privileged network position may be able to inject keystrokes by spoofing a keyboard

Description: The issue was addressed with improved checks.

CVE-2024-23277: Marc Newlin of SkySafe

ColorSync

Available for: macOS Sonoma

Impact: Processing a file may lead to unexpected app termination or arbitrary code execution

Description: The issue was addressed with improved memory handling.

CVE-2024-23247: m4yfly with TianGong Team of Legendsec at Qi'anxin Group

ColorSync

Available for: macOS Sonoma

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

Description: The issue was addressed with improved memory handling.

CVE-2024-23248: m4yfly with TianGong Team of Legendsec at Qi'anxin Group

CVE-2024-23249: m4yfly with TianGong Team of Legendsec at Qi'anxin Group

CoreBluetooth - LE

Available for: macOS Sonoma

Impact: An app may be able to access Bluetooth-connected microphones without user permission

Description: An access issue was addressed with improved access restrictions.

CVE-2024-23250: Guilherme Rambo of Best Buddy Apps (rambo.codes)

Disk Images

Available for: macOS Sonoma

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

Description: The issue was addressed with improved checks.

CVE-2024-23299: an anonymous researcher

Entry added May 29, 2024

Dock

Available for: macOS Sonoma

Impact: An app from a standard user account may be able to escalate privilege after admin user login

Description: A logic issue was addressed with improved restrictions.

CVE-2024-23244: Csaba Fitzl (@theevilbit) of OffSec

ExtensionKit

Available for: macOS Sonoma

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-2024-23205

file

Available for: macOS Sonoma

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

Description: This issue was addressed with improved checks.

CVE-2022-48554

Find My

Available for: macOS Sonoma

Impact: A malicious application may be able to access Find My data

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

CVE-2024-23229: Joshua Jewett (@JoshJewett33)

Entry added May 13, 2024

Foundation

Available for: macOS Sonoma

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

Description: A logic issue was addressed with improved checks.

CVE-2024-27789: Mickey Jin (@patch1t)

Entry added May 13, 2024

Image Capture

Available for: macOS Sonoma

Impact: An app may be able to access a user's Photos Library

Description: A permissions issue was addressed with additional restrictions.

CVE-2024-23253: Mickey Jin (@patch1t)

Image Processing

Available for: macOS Sonoma

Impact: An app may be able to execute arbitrary code with kernel privileges

Description: The issue was addressed with improved memory handling.

CVE-2024-23270: an anonymous researcher

ImageIO

Available for: macOS Sonoma

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

Description: The issue was addressed with improved memory handling.

CVE-2024-23257: Junsung Lee working with Trend Micro Zero Day Initiative

ImageIO

Available for: macOS Sonoma

Impact: Processing an image may lead to arbitrary code execution

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

CVE-2024-23258: Zhenjiang Zhao of pangu team, Qianxin, and Amir Bazine and Karsten König of CrowdStrike Counter Adversary Operations

Entry updated May 29, 2024

ImageIO

Available for: macOS Sonoma

Impact: Processing an image may lead to arbitrary code execution

Description: A buffer overflow issue was addressed with improved memory handling.

CVE-2024-23286: Junsung Lee working with Trend Micro Zero Day Initiative, Amir Bazine and Karsten König of CrowdStrike Counter Adversary Operations, Dohyun Lee (@l33d0hyun), and Lyutoon and Mr.R

Entry updated May 29, 2024

Intel Graphics Driver

Available for: macOS Sonoma

Impact: An app may be able to execute arbitrary code with kernel privileges

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

CVE-2024-23234: Murray Mike

Kerberos v5 PAM module

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-2024-23266: Pedro Tôrres (@t0rr3sp3dr0)

Kernel

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-2024-23235

Kernel

Available for: macOS Sonoma

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

Description: A memory corruption vulnerability was addressed with improved locking.

CVE-2024-23265: Xinru Chi of Pangu Lab

Kernel

Available for: macOS Sonoma

Impact: An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited.

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

CVE-2024-23225

libarchive

Available for: macOS Sonoma

Impact: A maliciously crafted ZIP archive may bypass Gatekeeper checks

Description: This issue was addressed with improved checks.

CVE-2024-27853: koocola

Entry added July 29, 2024

libxpc

Available for: macOS Sonoma

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

Description: The issue was addressed with improved checks.

CVE-2024-23278: an anonymous researcher

libxpc

Available for: macOS Sonoma

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

Description: The issue was addressed with improved memory handling.

CVE-2024-0258: ali yabuz

MediaRemote

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-2024-23279: an anonymous researcher

Messages

Available for: macOS Sonoma

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

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

CVE-2024-23287: Kirin (@Pwnrin)

Metal

Available for: macOS Sonoma

Impact: An application may be able to read restricted memory

Description: A validation issue was addressed with improved input sanitization.

CVE-2024-23264: Meysam Firouzi @R00tkitsmm working with Trend Micro Zero Day Initiative

Music

Available for: macOS Sonoma

Impact: An app may be able to create symlinks to protected regions of the disk

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

CVE-2024-23285: @08Tc3wBB of Jamf

Music

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-2024-27809: an anonymous researcher

Entry added July 29, 2024

Notes

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-2024-23283

NSSpellChecker

Available for: macOS Sonoma

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

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

CVE-2024-27887: Mickey Jin (@patch1t)

Entry added July 29, 2024

OpenSSH

Available for: macOS Sonoma

Impact: Multiple issues in OpenSSH

Description: Multiple issues were addressed by updating to OpenSSH 9.6.

CVE-2023-48795

CVE-2023-51384

CVE-2023-51385

PackageKit

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 state management.

CVE-2022-42816: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Sonoma

Impact: An app may be able to overwrite arbitrary files

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

CVE-2024-23216: Pedro Tôrres (@t0rr3sp3dr0)

PackageKit

Available for: macOS Sonoma

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

Description: The issue was addressed with improved checks.

CVE-2024-23267: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Sonoma

Impact: An app may be able to elevate privileges

Description: An injection issue was addressed with improved input validation.

CVE-2024-23268: Mickey Jin (@patch1t), Pedro Tôrres (@t0rr3sp3dr0)

CVE-2024-23274: Bohdan Stasiuk (@Bohdan_Stasiuk)

PackageKit

Available for: macOS Sonoma

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

Description: A logic issue was addressed with improved checks.

CVE-2023-42853: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Sonoma

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

Description: A race condition was addressed with additional validation.

CVE-2024-23275: Mickey Jin (@patch1t)

PackageKit

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 vulnerable code and adding additional checks.

CVE-2024-27888: Mickey Jin (@patch1t)

Entry added July 29, 2024

Photos

Available for: macOS Sonoma

Impact: Photos in the Hidden Photos Album may be viewed without authentication

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

CVE-2024-23255: Harsh Tyagi

QuartzCore

Available for: macOS Sonoma

Impact: Processing malicious input may lead to code execution

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

CVE-2024-23294: Wojciech Regula of SecuRing (wojciechregula.blog)

RTKit

Available for: macOS Sonoma

Impact: An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited.

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

CVE-2024-23296

Safari

Available for: macOS Sonoma

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

Description: The issue was addressed with improved checks.

CVE-2024-23259: Lyra Rebane (rebane2001)

Safari Private Browsing

Available for: macOS Sonoma

Impact: Private Browsing tabs may be accessed without authentication

Description: This issue was addressed through improved state management.

CVE-2024-23273: Matej Rabzelj

Sandbox

Available for: macOS Sonoma

Impact: An app may be able to edit NVRAM variables

Description: An access issue was addressed with improved access restrictions.

CVE-2024-23238

Sandbox

Available for: macOS Sonoma

Impact: An app may be able to leak sensitive user information

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

CVE-2024-23239: Mickey Jin (@patch1t)

Sandbox

Available for: macOS Sonoma

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

Description: A logic issue was addressed with improved restrictions.

CVE-2024-23290: Wojciech Regula of SecuRing (wojciechregula.blog)

Screen Capture

Available for: macOS Sonoma

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-2024-23232: Yiğit Can YILMAZ (@yilmazcanyigit)

Share Sheet

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-2024-23231: Kirin (@Pwnrin) and luckyu (@uuulucky)

SharedFileList

Available for: macOS Sonoma

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

Description: This issue was addressed with improved file handling.

CVE-2024-23230: Mickey Jin (@patch1t)

Shortcuts

Available for: macOS Sonoma

Impact: Third-party shortcuts may use a legacy action from Automator to send events to apps without user consent

Description: This issue was addressed by adding an additional prompt for user consent.

CVE-2024-23245: an anonymous researcher

Shortcuts

Available for: macOS Sonoma

Impact: An app may be able to access information about a user's contacts

Description: This issue was addressed with improved data protection.

CVE-2024-23292: K宝 and LFY@secsys from Fudan University

Siri

Available for: macOS Sonoma

Impact: A person with physical access to a device may be able to use Siri to access private calendar information

Description: A lock screen issue was addressed with improved state management.

CVE-2024-23289: Lewis Hardy

Siri

Available for: macOS Sonoma

Impact: An attacker with physical access may be able to use Siri to access sensitive user data

Description: This issue was addressed through improved state management.

CVE-2024-23293: Bistrit Dahal

Spotlight

Available for: macOS Sonoma

Impact: An app may be able to leak sensitive user information

Description: This issue was addressed through improved state management.

CVE-2024-23241

Storage Services

Available for: macOS Sonoma

Impact: An attacker may gain access to protected parts of the file system

Description: A logic issue was addressed with improved checks.

CVE-2024-23272: Mickey Jin (@patch1t)

Entry updated May 13, 2024

Synapse

Available for: macOS Sonoma

Impact: An app may be able to view Mail data

Description: A privacy issue was addressed by not logging contents of text fields.

CVE-2024-23242

System Settings

Available for: macOS Sonoma

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

Description: This issue was addressed with improved state management.

CVE-2024-23281: Joshua Jewett (@JoshJewett33)

TCC

Available for: macOS Sonoma

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

Description: This issue was addressed by adding an additional prompt for user consent.

CVE-2024-27792: Mickey Jin (@patch1t)

Entry added May 29, 2024

Time Zone

Available for: macOS Sonoma

Impact: An attacker may be able to read information belonging to another user

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

CVE-2024-23261: Matthew Loewen

Entry added July 29, 2024

TV App

Available for: macOS Sonoma

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

Description: This issue was addressed by removing additional entitlements.

CVE-2024-23260: Joshua Jewett (@JoshJewett33)

UIKit

Available for: macOS Sonoma

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

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

CVE-2024-23246: Deutsche Telekom Security GmbH sponsored by Bundesamt für Sicherheit in der Informationstechnik

WebKit

Available for: macOS Sonoma

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

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 263758

CVE-2024-54658: anbu1024 of SecANT

Entry added February 5, 2025

WebKit

Available for: macOS Sonoma

Impact: Processing web content may lead to arbitrary code execution

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 259694

CVE-2024-23226: Pwn2car

WebKit Bugzilla: 263001

CVE-2024-27859: Pwn2car

Entry added March 7, 2024, updated February 5, 2025

WebKit

Available for: macOS Sonoma

Impact: A malicious website may exfiltrate audio data cross-origin

Description: The issue was addressed with improved UI handling.

WebKit Bugzilla: 263795

CVE-2024-23254: James Lee (@Windowsrcer)

WebKit

Available for: macOS Sonoma

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

Description: A logic issue was addressed with improved validation.

WebKit Bugzilla: 264811

CVE-2024-23263: Johan Carlsson (joaxcar)

WebKit

Available for: macOS Sonoma

Impact: A maliciously crafted webpage may be able to fingerprint the user

Description: An injection issue was addressed with improved validation.

WebKit Bugzilla: 266703

CVE-2024-23280: an anonymous researcher

WebKit

Available for: macOS Sonoma

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

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

WebKit Bugzilla: 267241

CVE-2024-23284: Georg Felber and Marco Squarcina

Additional recognition

AppKit

We would like to acknowledge Stephan Casas and an anonymous researcher for their assistance.

Entry updated May 29, 2024

CoreAnimation

We would like to acknowledge Junsung Lee for their assistance.

CoreMotion

We would like to acknowledge Eric Dorphy of Twin Cities App Dev LLC for their assistance.

Endpoint Security

We would like to acknowledge Matthew White for their assistance.

Find My

We would like to acknowledge Meng Zhang (鲸落) of NorthSea for their assistance.

ICU

We would like to acknowledge Andr.Ess and an anonymous researcher for their assistance.

Entry added February 5, 2025

Kernel

We would like to acknowledge Tarek Joumaa (@tjkr0wn) and 이준성(Junsung Lee) for their assistance.

libxml2

We would like to acknowledge OSS-Fuzz, and Ned Williamson of Google Project Zero for their assistance.

libxpc

We would like to acknowledge Rasmus Sten, F-Secure (Mastodon: @pajp@blog.dll.nu), and an anonymous researcher for their assistance.

Messages

We would like to acknowledge Petar Mataić for their assistance.

Entry added February 5, 2025

Model I/O

We would like to acknowledge Junsung Lee for their assistance.

Photos

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) of Lakshmi Narain College Of Technology Bhopal for their assistance.

Power Management

We would like to acknowledge Pan ZhenPeng (@Peterpan0927) of STAR Labs SG Pte. Ltd. for their assistance.

Safari

We would like to acknowledge Abhinav Saraswat, Matthew C, and 이동하 (Lee Dong Ha of ZeroPointer Lab) for their assistance.

Sandbox

We would like to acknowledge Wojciech Regula of SecuRing (wojciechregula.blog) and Zhongquan Li (@Guluisacat) for their assistance.

Entry added July 29, 2024

SharedFileList

We would like to acknowledge Phil Schneider of Canva for their assistance.

Shortcuts

We would like to acknowledge Yusuf Kelany for their assistance.

Entry added July 29, 2024

Siri

We would like to acknowledge Bistrit Dahal for their assistance.

Storage Driver

We would like to acknowledge Liang Wei of PixiePoint Security for their assistance.

SystemMigration

We would like to acknowledge Eugene Gershnik for their assistance.

TCC

We would like to acknowledge Mickey Jin (@patch1t) for their assistance.

WebKit

We would like to acknowledge Nan Wang (@eternalsakura13) of 360 Vulnerability Research Institute, Valentino Dalla Valle, Pedro Bernardo, Marco Squarcina, and Lorenzo Veronese of TU Wien for their assistance.

WebRTC

We would like to acknowledge Narendra Bhati From Suma Soft Pvt. Ltd, Pune (India) - twitter.com/imnarendrabhati for their assistance.

Entry added February 5, 2025

XProtect

We would like to acknowledge Koh M. Nakagawa (@tsunek0h) for their assistance.

Entry added February 5, 2025

Published Date: February 05, 2025