About the security content of macOS Ventura 13.6.5

This document describes the security content of macOS Ventura 13.6.5.

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 Ventura 13.6.5

Released March 7, 2024

Admin Framework

Available for: macOS Ventura

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 Ventura

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

AppleMobileFileIntegrity

Available for: macOS Ventura

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)

ColorSync

Available for: macOS Ventura

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

CoreCrypto

Available for: macOS Ventura

Impact: An attacker may be able to decrypt legacy RSA PKCS#1 v1.5 ciphertexts without having the private key

Description: A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions.

CVE-2024-23218: Clemens Lang

Disk Images

Available for: macOS Ventura

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 31, 2024

Find My

Available for: macOS Ventura

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

Image Processing

Available for: macOS Ventura

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 Ventura

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 31, 2024

ImageIO

Available for: macOS Ventura

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

Intel Graphics Driver

Available for: macOS Ventura

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 Ventura

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 Ventura

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 Ventura

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

libxpc

Available for: macOS Ventura

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2024-23201: Koh M. Nakagawa of FFRI Security, Inc., an anonymous researcher

libxpc

Available for: macOS Ventura

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

MediaRemote

Available for: macOS Ventura

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

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

CVE-2023-28826: Meng Zhang (鲸落) of NorthSea

Metal

Available for: macOS Ventura

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

Notes

Available for: macOS Ventura

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

PackageKit

Available for: macOS Ventura

Impact: An app may be able to elevate privileges

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

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

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

PackageKit

Available for: macOS Ventura

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 Ventura

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 Ventura

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)

Share Sheet

Available for: macOS Ventura

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 Ventura

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 Ventura

Impact: A shortcut may be able to use sensitive data with certain actions without prompting the user

Description: The issue was addressed with additional permissions checks.

CVE-2024-23203: an anonymous researcher

CVE-2024-23204: Jubaer Alnazi (@h33tjubaer)

Shortcuts

Available for: macOS Ventura

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 Ventura

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

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

CVE-2024-23217: Kirin (@Pwnrin)

Storage Services

Available for: macOS Ventura

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

Transparency

Available for: macOS Ventura

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

Description: The issue was addressed with improved restriction of data container access.

CVE-2023-40389: Csaba Fitzl (@theevilbit) of Offensive Security and Joshua Jewett (@JoshJewett33)

Entry added May 31, 2024

Additional recognition

Messages

We would like to acknowledge Petar Mataić for their assistance.

Entry added February 5, 2025

Published Date: February 13, 2025