

About the security content of macOS Monterey 12.4

This document describes the security content of macOS Monterey 12.4.

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 updates](#) page.

Apple security documents reference vulnerabilities by [CVE-ID](#) when possible.

For more information about security, see the [Apple Product Security](#) page.

macOS Monterey 12.4

Released May 16, 2022

AMD

Available for: macOS Monterey

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

Description: A memory corruption issue was addressed with improved state management.

CVE-2022-26772: an anonymous researcher

AMD

Available for: macOS Monterey

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

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

CVE-2022-26741: ABC Research s.r.o

CVE-2022-26742: ABC Research s.r.o

CVE-2022-26749: ABC Research s.r.o

CVE-2022-26750: ABC Research s.r.o

CVE-2022-26752: ABC Research s.r.o

CVE-2022-26753: ABC Research s.r.o

CVE-2022-26754: ABC Research s.r.o

apache

Available for: macOS Monterey

Impact: Multiple issues in apache

Description: Multiple issues were addressed by updating apache to version 2.4.53.

CVE-2021-44224

CVE-2021-44790

CVE-2022-22719

CVE-2022-22720

CVE-2022-22721

AppleGraphicsControl

Available for: macOS Monterey

Impact: Processing a maliciously crafted image may lead to arbitrary code execution

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

CVE-2022-26751: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

AppleMobileFileIntegrity

Available for: macOS Monterey

Impact: A user may be able to view sensitive user information

Description: An issue in the handling of environment variables was addressed with improved validation.

CVE-2022-26707: Wojciech Reguła (@_r3ggi) of SecuRing

Entry added July 6, 2022

AppleScript

Available for: macOS Monterey

Impact: Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory

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

CVE-2022-26697: Qi Sun and Robert Ai of Trend Micro

AppleScript

Available for: macOS Monterey

Impact: Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory

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

CVE-2022-26698: Qi Sun of Trend Micro, Ye Zhang (@co0py_Cat) of Baidu Security

Entry updated July 6, 2022

AVEVideoEncoder

Available for: macOS Monterey

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

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

CVE-2022-26736: an anonymous researcher

CVE-2022-26737: an anonymous researcher

CVE-2022-26738: an anonymous researcher

CVE-2022-26739: an anonymous researcher

CVE-2022-26740: an anonymous researcher

Bluetooth

Available for: macOS Monterey

Impact: An app may gain unauthorized access to Bluetooth

Description: A logic issue was addressed with improved checks.

CVE-2022-32783: Jon Thompson of Evolve (Des Moines, IA)

Entry added July 6, 2022

Contacts

Available for: macOS Monterey

Impact: A plug-in may be able to inherit the application's permissions and access user data

Description: This issue was addressed with improved checks.

CVE-2022-26694: Wojciech Reguła (@_r3ggi) of SecuRing

CVMS

Available for: macOS Monterey

Impact: A malicious application may be able to gain root privileges

Description: A memory initialization issue was addressed.

CVE-2022-26721: Yonghwi Jin (@jinmo123) of Theori

CVE-2022-26722: Yonghwi Jin (@jinmo123) of Theori

DriverKit

Available for: macOS Monterey

Impact: A malicious application may be able to execute arbitrary code with system privileges

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

CVE-2022-26763: Linus Henze of Pinauten GmbH (pinauten.de)

FaceTime

Available for: macOS Monterey

Impact: An app with root privileges may be able to access private information

Description: This issue was addressed by enabling hardened runtime.

CVE-2022-32781: Wojciech Reguła (@_r3ggi) of SecuRing

Entry added July 6, 2022

ImageIO

Available for: macOS Monterey

Impact: A remote attacker may be able to cause unexpected application termination or arbitrary code execution

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

CVE-2022-26711: actae0n of Blacksun Hackers Club working with Trend Micro Zero Day Initiative

ImageIO

Available for: macOS Monterey

Impact: Photo location information may persist after it is removed with Preview Inspector

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

CVE-2022-26725: Andrew Williams and Avi Drissman of Google

Intel Graphics Driver

Available for: macOS Monterey

Impact: A malicious application may be able to execute arbitrary code with kernel privileges

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

CVE-2022-26720: Liu Long of Ant Security Light-Year Lab

Intel Graphics Driver

Available for: macOS Monterey

Impact: A malicious application may be able to execute arbitrary code with kernel privileges

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

CVE-2022-26769: Antonio Zekic (@antoniozekic)

Intel Graphics Driver

Available for: macOS Monterey

Impact: A malicious application may be able to execute arbitrary code with kernel privileges

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

CVE-2022-26770: Liu Long of Ant Security Light-Year Lab

Intel Graphics Driver

Available for: macOS Monterey

Impact: Processing maliciously crafted web content may lead to arbitrary code execution

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

CVE-2022-26748: Jeonghoon Shin of Theori working with Trend Micro Zero Day Initiative

Intel Graphics Driver

Available for: macOS Monterey

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

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

CVE-2022-26756: Jack Dates of RET2 Systems, Inc

IOKit

Available for: macOS Monterey

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

Description: A race condition was addressed with improved locking.

CVE-2022-26701: chenyuwang (@mzzzz_) of Tencent Security Xuanwu Lab

IOMobileFrameBuffer

Available for: macOS Monterey

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

Description: A memory corruption issue was addressed with improved state management.

CVE-2022-26768: an anonymous researcher

Kernel

Available for: macOS Monterey

Impact: A malicious application may cause unexpected changes in memory shared between processes

Description: A memory corruption issue was addressed with improved state management.

CVE-2022-26758: an anonymous researcher

Entry added October 31, 2023

Kernel

Available for: macOS Monterey

Impact: An attacker that has already achieved code execution in macOS Recovery may be able to escalate to kernel privileges

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

CVE-2022-26743: Jordy Zomer (@pwningsystems)

Kernel

Available for: macOS Monterey

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

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

CVE-2022-26714: Peter Nguyễn Vũ Hoàng (@peternguyen14) of STAR Labs (@starlabs_sg)

Kernel

Available for: macOS Monterey

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

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

CVE-2022-26757: Ned Williamson of Google Project Zero

Kernel

Available for: macOS Monterey

Impact: An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations

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

CVE-2022-26764: Linus Henze of Pinauten GmbH (pinauten.de)

Kernel

Available for: macOS Monterey

Impact: A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication

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

CVE-2022-26765: Linus Henze of Pinauten GmbH (pinauten.de)

LaunchServices

Available for: macOS Monterey

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

Description: An access issue was addressed with additional sandbox restrictions on third-party applications.

CVE-2022-26706: Arsenii Kostromin (0x3c3e), Jonathan Bar Or of Microsoft

Entry updated July 6, 2022

LaunchServices

Available for: macOS Monterey

Impact: A malicious application may be able to bypass Privacy preferences

Description: The issue was addressed with additional permissions checks.

CVE-2022-26767: Wojciech Reguła (@_r3ggi) of SecuRing

Libinfo

Available for: macOS Monterey

Impact: An app may be able to bypass Privacy preferences

Description: This issue was addressed with improved checks.

CVE-2022-32882: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020) of Tencent Security Xuanwu Lab

Entry added September 16, 2022

libresolv

Available for: macOS Monterey

Impact: A remote user may be able to cause a denial-of-service

Description: This issue was addressed with improved checks.

CVE-2022-32790: Max Shavrick (@_mxms) of the Google Security Team

Entry added June 21, 2022

libresolv

Available for: macOS Monterey

Impact: An attacker may be able to cause unexpected application termination or arbitrary code execution

Description: This issue was addressed with improved checks.

CVE-2022-26776: Zubair Ashraf of CrowdStrike, Max Shavrick (@_mxms) of the Google Security Team

CVE-2022-26708: Max Shavrick (@_mxms) of the Google Security Team

libresolv

Available for: macOS Monterey

Impact: An attacker may be able to cause unexpected application termination or arbitrary code execution

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

CVE-2022-26775: Max Shavrick (@_mxms) of the Google Security Team

LibreSSL

Available for: macOS Monterey

Impact: Processing a maliciously crafted certificate may lead to a denial of service

Description: A denial of service issue was addressed with improved input validation.

CVE-2022-0778

libxml2

Available for: macOS Monterey

Impact: A remote attacker may be able to cause unexpected application termination or arbitrary code execution

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

CVE-2022-23308

Login Window

Available for: macOS Monterey

Impact: A person with access to a Mac may be able to bypass Login Window

Description: A consistency issue was addressed with improved state handling.

CVE-2022-48575: Paul Walker of Bury and Nathaniel Ekoniak of Ennate Technologies

Entry added October 31, 2023

OpenSSL

Available for: macOS Monterey

Impact: Processing a maliciously crafted certificate may lead to a denial of service

Description: This issue was addressed with improved checks.

CVE-2022-0778

PackageKit

Available for: macOS Monterey

Impact: An app may be able to gain elevated privileges

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

CVE-2022-32794: Mickey Jin (@patch1t)

Entry added October 4, 2022

PackageKit

Available for: macOS Monterey

Impact: An application may be able to gain elevated privileges

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

CVE-2022-22617: Mickey Jin (@patch1t)

Entry added July 6, 2022

PackageKit

Available for: macOS Monterey

Impact: A malicious application may be able to modify protected parts of the file system

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

CVE-2022-26712: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Monterey

Impact: A malicious application may be able to modify protected parts of the file system

Description: This issue was addressed with improved entitlements.

CVE-2022-26727: Mickey Jin (@patch1t)

Photo Booth

Available for: macOS Monterey

Impact: An app with root privileges may be able to access private information

Description: This issue was addressed by enabling hardened runtime.

CVE-2022-32782: Wojciech Reguła (@_r3ggi) of SecuRing

Entry added July 6, 2022

Preview

Available for: macOS Monterey

Impact: A plug-in may be able to inherit the application's permissions and access user data

Description: This issue was addressed with improved checks.

CVE-2022-26693: Wojciech Reguła (@_r3ggi) of SecuRing

Printing

Available for: macOS Monterey

Impact: A malicious application may be able to bypass Privacy preferences

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

CVE-2022-26746: @gorelics

Safari Private Browsing

Available for: macOS Monterey

Impact: A malicious website may be able to track users in Safari private browsing mode

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

CVE-2022-26731: an anonymous researcher

Security

Available for: macOS Monterey

Impact: A malicious app may be able to bypass signature validation

Description: A certificate parsing issue was addressed with improved checks.

CVE-2022-26766: Linus Henze of Pinauten GmbH (pinauten.de)

SMB

Available for: macOS Monterey

Impact: An application may be able to gain elevated privileges

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

CVE-2022-26715: Peter Nguyễn Vũ Hoàng of STAR Labs

SMB

Available for: macOS Monterey

Impact: An application may be able to gain elevated privileges

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

CVE-2022-26718: Peter Nguyễn Vũ Hoàng of STAR Labs

SMB

Available for: macOS Monterey

Impact: Mounting a maliciously crafted Samba network share may lead to arbitrary code execution

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

CVE-2022-26723: Felix Poulin-Belanger

SoftwareUpdate

Available for: macOS Monterey

Impact: A malicious application may be able to access restricted files

Description: This issue was addressed with improved entitlements.

CVE-2022-26728: Mickey Jin (@patch1t)

Spotlight

Available for: macOS Monterey

Impact: An app may be able to gain elevated privileges

Description: A validation issue existed in the handling of symlinks and was addressed with improved validation of symlinks.

CVE-2022-26704: Gergely Kalman (@gergely_kalman), and Joshua Mason of Mandiant

Entry updated October 31, 2023

System Preferences

Available for: macOS Monterey

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

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

CVE-2022-42857: Mickey Jin (@patch1t)

Entry added October 31, 2023

TCC

Available for: macOS Monterey

Impact: An app may be able to capture a user's screen

Description: This issue was addressed with improved checks.

CVE-2022-26726: Antonio Cheong Yu Xuan of YCISCQ

Entry updated May 11, 2023

Tcl

Available for: macOS Monterey

Impact: A malicious application may be able to break out of its sandbox

Description: This issue was addressed with improved environment sanitization.

CVE-2022-26755: Arsenii Kostromin (0x3c3e)

Terminal

Available for: macOS Monterey

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

Description: This issue was addressed with improved environment sanitization.

CVE-2022-26696: Ron Waisberg, an anonymous researcher, Wojciech Reguła (@_r3ggi) of SecuRing, and Ron Hass (@ronhass7) of Perception Point

Entry added September 16, 2022, updated October 31, 2023

WebKit

Available for: macOS Monterey

Impact: Processing maliciously crafted web content may lead to code execution

Description: A memory corruption issue was addressed with improved state management.

WebKit Bugzilla: 238178

CVE-2022-26700: ryuzaki

WebKit

Available for: macOS Monterey

Impact: Processing maliciously crafted web content may lead to arbitrary code execution

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

WebKit Bugzilla: 236950

CVE-2022-26709: Chijin Zhou of ShuiMuYuLin Ltd and Tsinghua wingtecher lab

WebKit Bugzilla: 237475

CVE-2022-26710: Chijin Zhou of ShuiMuYuLin Ltd and Tsinghua wingtecher lab

WebKit Bugzilla: 238171

CVE-2022-26717: Jeonghoon Shin of Theori

WebKit

Available for: macOS Monterey

Impact: Processing maliciously crafted web content may lead to arbitrary code execution

Description: A memory corruption issue was addressed with improved state management.

WebKit Bugzilla: 238183

CVE-2022-26716: SorryMybad (@S0rryMybad) of Kunlun Lab

WebKit Bugzilla: 238699

CVE-2022-26719: Dongzhuo Zhao working with ADLab of Venustech

WebRTC

Available for: macOS Monterey

Impact: Video self-preview in a webRTC call may be interrupted if the user answers a phone call

Description: A logic issue in the handling of concurrent media was addressed with improved state handling.

WebKit Bugzilla: 237524

CVE-2022-22677: an anonymous researcher

Wi-Fi

Available for: macOS Monterey

Impact: A malicious application may disclose restricted memory

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

CVE-2022-26745: Scarlet Raine

Entry updated July 6, 2022

Wi-Fi

Available for: macOS Monterey

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

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

CVE-2022-26761: Wang Yu of Cyberserval

Wi-Fi

Available for: macOS Monterey

Impact: A malicious application may be able to execute arbitrary code with system privileges

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

CVE-2022-26762: Wang Yu of Cyberserval

zip

Available for: macOS Monterey

Impact: Processing a maliciously crafted file may lead to a denial of service

Description: A denial of service issue was addressed with improved state handling.

CVE-2022-0530

zlib

Available for: macOS Monterey

Impact: An attacker may be able to cause unexpected application termination or arbitrary code execution

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

CVE-2018-25032: Tavis Ormandy

zsh

Available for: macOS Monterey

Impact: A remote attacker may be able to cause arbitrary code execution

Description: This issue was addressed by updating to zsh version 5.8.1.

CVE-2021-45444

Additional recognition

AppleMobileFileIntegrity

We would like to acknowledge Wojciech Reguła (@_r3ggi) of SecuRing for their assistance.

Bluetooth

We would like to acknowledge Jann Horn of Project Zero for their assistance.

Calendar

We would like to acknowledge Eugene Lim of Government Technology Agency of Singapore for their assistance.

FaceTime

We would like to acknowledge Wojciech Reguła (@_r3ggi) of SecuRing for their assistance.

FileVault

We would like to acknowledge Benjamin Adolphi of Promon Germany GmbH for their assistance.

Login Window

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

Photo Booth

We would like to acknowledge Wojciech Reguła (@_r3ggi) of SecuRing for their assistance.

System Preferences

We would like to acknowledge Mohammad Tausif Siddiqui (@toshsiddiqui), Victor Grinchik (grinchik.com), and an anonymous researcher for their assistance.

Entry updated October 31, 2023

WebKit

We would like to acknowledge James Lee and an anonymous researcher for their assistance.

Entry updated May 25, 2022

Wi-Fi

We would like to acknowledge Dana Morrison 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: August 20, 2024

Helpful?

Yes

No

 > Support > About the security content of macOS Monterey 12.4

Copyright © 2026 Apple Inc. All rights reserved. [Privacy Policy](#) | [Terms of Use](#) | [Sales and Refunds](#) | [Site Map](#)

United States