



Site Search

[Full Disclosure](#) mailing list archives[← By Date →](#) [← By Thread →](#)

List Archive Search



APPLE-SA-2022-05-16-2 macOS Monterey 12.4

From: Apple Product Security via Fulldisclosure <fulldisclosure () seclists org>

Date: Mon, 16 May 2022 16:20:15 -0700

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

APPLE-SA-2022-05-16-2 macOS Monterey 12.4

macOS Monterey 12.4 addresses the following issues.
Information about the security content is also available at
<https://support.apple.com/HT213257>.

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

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

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

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)

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: 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)

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

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

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: 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)

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: an anonymous researcher

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: an anonymous researcher

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)

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: an anonymous researcher

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), an anonymous researcher for their assistance.

WebKit

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

Wi-Fi

We would like to acknowledge Dana Morrison for their assistance.

macOS Monterey 12.4 may be obtained from the Mac App Store or Apple's Software Downloads web site: <https://support.apple.com/downloads/> All information is also posted on the Apple Security Updates web site: <https://support.apple.com/en-us/HT201222>.

This message is signed with Apple's Product Security PGP key, and details are available at: <https://www.apple.com/support/security/pgp/>

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAAdFiEEePiLW1MrMjw19XzoeC9qKD1prhgFAmKC1TUACgkQeC9qKD1p rhigoQ/cTnCM0Yau+v06pv8PHMbeEWPPvtsGpemCNz4iChXRhVOHKxgMQAHEgg EjpXvw5D1jg12wroXypL8AD0D1V200A7u5A20Lip1NIDL145692jPfmGuNxqkRnI DyoykhUogRL8Yvzkd5P8D3Jlo0EzCa4Zh04tqBwbrGQZRb7gHcLMPtzlgt15ZIma mH42QGRkJcK8v4MWNixvibnQPwx3we2k4T8FajBvoCxYinM0lg/j16hFREj8Src+ rQwKPV6JHiBBQ3LQpGeBlJrFLH72CyHbCu8IqWfYvvdXsT5Gr9JoagW7+g/9+8Wc 402HjkY4w0ZrxIBtlaUlNFZuB1mtIv8amHn9AaV0K/7GALSP6MQzA+U3HUqd3hYV J23pw6iRWBTZZSm031kdEGU/X9uDkDKJL6QxUfzVXPVm0s0VNMmOJUdTRKf3tdsa 5qnPcjowRONgltX8NqIP0q4aJPr1WigtFGyASIr3me/t9Ft7Kss4gJt7YLDsN6MZ opD8hTRHSAXAAYsA57omyo/DnmajHIbUGVEujzAh/DOEYxgT9aaaAHnkNuaQgIbs Z5g/dfhDaJodyk0q7BIeK+RPbkvrJvnoBwKrnAUaSgYMX14DQdExLBEvbpPg71f LHzULUewIuuP/57huTz/b4vEEke0JUwrWk6T1ACbndL3FsPI0X4= =jaCZ

-----END PGP SIGNATURE-----

Sent through the Full Disclosure mailing list <https://nmap.org/mailman/listinfo/fulldisclosure> Web Archives & RSS: <https://seclists.org/fulldisclosure/>

◀ [By Date](#) ▶ ◀ [By Thread](#) ▶

Current thread:

APPLE-SA-2022-05-16-2 macOS Monterey 12.4 Apple Product Security via Fulldisclosure (May 16)

Site Search



Nmap Security Scanner

Npcap packet capture

Security Lists

Security Tools

About

Ref Guide

User's Guide

Nmap Announce

Vuln scanners

About/Contact

Install Guide

API docs

Nmap Dev

Password audit

Privacy

Docs

Download

Full Disclosure

Web scanners

Advertising

Download

Npcap OEM

Open Source Security

Wireless

Nmap Public Source License

Nmap OEM

BreachExchange

Exploitation



