About the security content of macOS Tahoe 26.4

This document describes the security content of macOS Tahoe 26.4.

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 Tahoe 26.4

Released March 24, 2026

802.1X

Available for: macOS Tahoe

Impact: An attacker in a privileged network position may be able to intercept network traffic

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

CVE-2026-28865: Héloïse Gollier and Mathy Vanhoef (KU Leuven)

Accounts

Available for: macOS Tahoe

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

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

CVE-2026-28877: Rosyna Keller of Totally Not Malicious Software

Admin Framework

Available for: macOS Tahoe

Impact: An app with root privileges may be able to delete protected system files

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

CVE-2026-28823: Ryan Dowd (@_rdowd)

apache

Available for: macOS Tahoe

Impact: Multiple issues in Apache

Description: This is a vulnerability in open source code and Apple Software is among the affected projects. The CVE-ID was assigned by a third party. Learn more about the issue and CVE-ID at cve.org.

CVE-2025-55753

CVE-2025-58098

CVE-2025-59775

CVE-2025-65082

CVE-2025-66200

AppleMobileFileIntegrity

Available for: macOS Tahoe

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

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

CVE-2026-28824: Mickey Jin (@patch1t)

AppleMobileFileIntegrity

Available for: macOS Tahoe

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

Description: A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions.

CVE-2026-20699: Mickey Jin (@patch1t)

AppleScript

Available for: macOS Tahoe

Impact: An app may bypass Gatekeeper checks

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-20684: Koh M. Nakagawa (@tsunek0h) of FFRI Security, Inc.

Archive Utility

Available for: macOS Tahoe

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

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

CVE-2026-20633: Mickey Jin (@patch1t)

Audio

Available for: macOS Tahoe

Impact: Processing maliciously crafted web content may lead to an unexpected process crash

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

CVE-2026-28879: Justin Cohen of Google

Audio

Available for: macOS Tahoe

Impact: An attacker may be able to cause unexpected app termination

Description: A type confusion issue was addressed with improved memory handling.

CVE-2026-28822: Jex Amro

Calling Framework

Available for: macOS Tahoe

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

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

CVE-2026-28894: an anonymous researcher

Clipboard

Available for: macOS Tahoe

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

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

CVE-2026-28866: Cristian Dinca (icmd.tech)

CoreMedia

Available for: macOS Tahoe

Impact: Processing an audio stream in a maliciously crafted media file may terminate the process

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

CVE-2026-20690: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreServices

Available for: macOS Tahoe

Impact: An app may be able to gain elevated privileges

Description: A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement.

CVE-2026-28821: YingQi Shi (@Mas0nShi) of DBAppSecurity's WeBin lab

CoreServices

Available for: macOS Tahoe

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

Description: A permissions issue was addressed with additional sandbox restrictions.

CVE-2026-28838: an anonymous researcher

CoreUtils

Available for: macOS Tahoe

Impact: A user in a privileged network position may be able to cause a denial-of-service

Description: A null pointer dereference was addressed with improved input validation.

CVE-2026-28886: Etienne Charron (Renault) and Victoria Martini (Renault)

Crash Reporter

Available for: macOS Tahoe

Impact: An app may be able to enumerate a user's installed apps

Description: A privacy issue was addressed by removing sensitive data.

CVE-2026-28878: Zhongcheng Li from IES Red Team

CUPS

Available for: macOS Tahoe

Impact: An app may be able to gain root privileges

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

CVE-2026-28888: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

CUPS

Available for: macOS Tahoe

Impact: A document may be written to a temporary file when using print preview

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

CVE-2026-28893: Asaf Cohen

curl

Available for: macOS Tahoe

Impact: An issue existed in curl which may result in unintentionally sending sensitive information via an incorrect connection

Description: This is a vulnerability in open source code and Apple Software is among the affected projects. The CVE-ID was assigned by a third party. Learn more about the issue and CVE-ID at cve.org.

CVE-2025-14524

DeviceLink

Available for: macOS Tahoe

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

Description: A parsing issue in the handling of directory paths was addressed with improved path validation.

CVE-2026-28876: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

Diagnostics

Available for: macOS Tahoe

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

Description: A permissions issue was addressed by removing the vulnerable code.

CVE-2026-28892: 风沐云烟 (@binary_fmyy) and Minghao Lin (@Y1nKoc)

File System

Available for: macOS Tahoe

Impact: An app may be able to disclose kernel memory

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

CVE-2026-28832: DARKNAVY (@DarkNavyOrg)

GeoServices

Available for: macOS Tahoe

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

Description: An information leakage was addressed with additional validation.

CVE-2026-28870: XiguaSec

GPU Drivers

Available for: macOS Tahoe

Impact: An app may be able to cause unexpected system termination

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

CVE-2026-28834: an anonymous researcher

iCloud

Available for: macOS Tahoe

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

Description: A privacy issue was addressed by moving sensitive data.

CVE-2026-28881: Ye Zhang of Baidu Security, Ryan Dowd (@_rdowd), Csaba Fitzl (@theevilbit) of Iru

iCloud

Available for: macOS Tahoe

Impact: An app may be able to enumerate a user's installed apps

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-28880: Zhongcheng Li from IES Red Team

CVE-2026-28833: Zhongcheng Li from IES Red Team

ImageIO

Available for: macOS Tahoe

Impact: Processing a maliciously crafted file may lead to unexpected app termination

Description: This is a vulnerability in open source code and Apple Software is among the affected projects. The CVE-ID was assigned by a third party. Learn more about the issue and CVE-ID at cve.org.

CVE-2025-64505

IOGraphics

Available for: macOS Tahoe

Impact: A buffer overflow may result in memory corruption and unexpected app termination

Description: The issue was addressed with improved bounds checks.

CVE-2026-28842: Joseph Ravichandran (@0xjprx) of MIT CSAIL

IOGraphics

Available for: macOS Tahoe

Impact: A buffer overflow may result in memory corruption and unexpected app termination

Description: A buffer overflow was addressed with improved size validation.

CVE-2026-28841: Joseph Ravichandran (@0xjprx) of MIT CSAIL

Kernel

Available for: macOS Tahoe

Impact: An app may be able to disclose kernel memory

Description: A logging issue was addressed with improved data redaction.

CVE-2026-28868: 이동하 (Lee Dong Ha of BoB 0xB6)

Kernel

Available for: macOS Tahoe

Impact: An app may be able to leak sensitive kernel state

Description: This issue was addressed with improved authentication.

CVE-2026-28867: Jian Lee (@speedyfriend433)

Kernel

Available for: macOS Tahoe

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-2026-20698: DARKNAVY (@DarkNavyOrg)

Kernel

Available for: macOS Tahoe

Impact: An app may be able to determine kernel memory layout

Description: An information disclosure issue was addressed with improved memory management.

CVE-2026-20695: 이동하 (Lee Dong Ha of BoB 0xB6) working with TrendAI Zero Day Initiative, hari shanmugam

Kernel

Available for: macOS Tahoe

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

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

CVE-2026-20687: Johnny Franks (@zeroxjf)

LaunchServices

Available for: macOS Tahoe

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

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

CVE-2026-28845: Yuebin Sun (@yuebinsun2020), an anonymous researcher, Nathaniel Oh (@calysteon), Kirin (@Pwnrin), Wojciech Regula of SecuRing (wojciechregula.blog), Joshua Jewett (@JoshJewett33), an anonymous researcher

libxpc

Available for: macOS Tahoe

Impact: An app may be able to enumerate a user's installed apps

Description: This issue was addressed with improved checks.

CVE-2026-28882: Ilias Morad (A2nkF) of Voynich Group, Duy Trần (@khanhduytran0), @hugeBlack

libxpc

Available for: macOS Tahoe

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-20607: an anonymous researcher

Mail

Available for: macOS Tahoe

Impact: "Hide IP Address" and "Block All Remote Content" may not apply to all mail content

Description: A privacy issue was addressed with improved handling of user preferences.

CVE-2026-20692: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

MigrationKit

Available for: macOS Tahoe

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

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

CVE-2026-20694: Rodolphe Brunetti (@eisw0lf) of Lupus Nova

Music

Available for: macOS Tahoe

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

Description: A parsing issue in the handling of directory paths was addressed with improved path validation.

CVE-2026-20632: Rodolphe Brunetti (@eisw0lf) of Lupus Nova

NetAuth

Available for: macOS Tahoe

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

Description: The issue was addressed with improved checks.

CVE-2026-28839: Mickey Jin (@patch1t)

NetAuth

Available for: macOS Tahoe

Impact: An app may be able to connect to a network share without user consent

Description: An access issue was addressed with additional sandbox restrictions.

CVE-2026-20701: Matej Moravec (@MacejkoMoravec)

NetAuth

Available for: macOS Tahoe

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

Description: A race condition was addressed with additional validation.

CVE-2026-28891: an anonymous researcher

NetFSFramework

Available for: macOS Tahoe

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

Description: A parsing issue in the handling of directory paths was addressed with improved path validation.

CVE-2026-28827: Csaba Fitzl (@theevilbit) of Iru, an anonymous researcher

Notes

Available for: macOS Tahoe

Impact: An app may be able to delete files for which it does not have permission

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

CVE-2026-28816: Dawuge of Shuffle Team and Hunan University

NSColorPanel

Available for: macOS Tahoe

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

Description: A logic issue was addressed with improved restrictions.

CVE-2026-28826: an anonymous researcher

PackageKit

Available for: macOS Tahoe

Impact: A user may be able to elevate privileges

Description: A logic issue was addressed with improved checks.

CVE-2026-20631: Gergely Kalman (@gergely_kalman)

PackageKit

Available for: macOS Tahoe

Impact: An attacker with root privileges may be able to delete protected system files

Description: This issue was addressed through improved state management.

CVE-2026-20693: Mickey Jin (@patch1t)

Phone

Available for: macOS Tahoe

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-2026-28862: Kun Peeks (@SwayZGl1tZyyy)

Printing

Available for: macOS Tahoe

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

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

CVE-2026-28831: an anonymous researcher

Printing

Available for: macOS Tahoe

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

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

CVE-2026-28817: Gyujeong Jin (@G1uN4sh) at Team.0xb6

Printing

Available for: macOS Tahoe

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

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

CVE-2026-20688: wdszzml and Atuin Automated Vulnerability Discovery Engine

Security

Available for: macOS Tahoe

Impact: A local attacker may gain access to user's Keychain items

Description: This issue was addressed with improved permissions checking.

CVE-2026-28864: Alex Radocea

SMB

Available for: macOS Tahoe

Impact: Mounting a maliciously crafted SMB network share may lead to system termination

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

CVE-2026-28835: Christian Kohlschütter

SMB

Available for: macOS Tahoe

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

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

CVE-2026-28825: Sreejith Krishnan R

Spotlight

Available for: macOS Tahoe

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

Description: A logging issue was addressed with improved data redaction.

CVE-2026-28818: @pixiepointsec

Spotlight

Available for: macOS Tahoe

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-20697: @pixiepointsec

StorageKit

Available for: macOS Tahoe

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

Description: This issue was addressed with improved checks.

CVE-2026-28820: Mickey Jin (@patch1t)

System Settings

Available for: macOS Tahoe

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

Description: A logic issue was addressed with improved checks.

CVE-2026-28837: Luke Roberts (@rookuu)

SystemMigration

Available for: macOS Tahoe

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

Description: A file access issue was addressed with improved input validation.

CVE-2026-28844: Pedro Tôrres (@t0rr3sp3dr0)

TCC

Available for: macOS Tahoe

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

Description: A permissions issue was addressed by removing the vulnerable code.

CVE-2026-28828: Mickey Jin (@patch1t)

UIFoundation

Available for: macOS Tahoe

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

Description: A stack overflow was addressed with improved input validation.

CVE-2026-28852: Caspian Tarafdar

WebDAV

Available for: macOS Tahoe

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-28829: Sreejith Krishnan R

WebKit

Available for: macOS Tahoe

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

Description: This issue was addressed through improved state management.

WebKit Bugzilla: 304951

CVE-2026-20665: webb

WebKit

Available for: macOS Tahoe

Impact: Processing maliciously crafted web content may bypass Same Origin Policy

Description: A cross-origin issue in the Navigation API was addressed with improved input validation.

WebKit Bugzilla: 306050

CVE-2026-20643: Thomas Espach

WebKit

Available for: macOS Tahoe

Impact: Visiting a maliciously crafted website may lead to a cross-site scripting attack

Description: A logic issue was addressed with improved checks.

WebKit Bugzilla: 305859

CVE-2026-28871: @hamayanhamayan

WebKit

Available for: macOS Tahoe

Impact: Processing maliciously crafted web content may lead to an unexpected process crash

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 306136

CVE-2026-20664: Daniel Rhea, Söhnke Benedikt Fischedick (Tripton), Emrovsky & Switch, Yevhen Pervushyn

WebKit Bugzilla: 307723

CVE-2026-28857: Narcis Oliveras Fontàs, Söhnke Benedikt Fischedick (Tripton), Daniel Rhea, Nathaniel Oh (@calysteon)

WebKit

Available for: macOS Tahoe

Impact: A malicious website may be able to access script message handlers intended for other origins

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

WebKit Bugzilla: 307014

CVE-2026-28861: Hongze Wu and Shuaike Dong from Ant Group Infrastructure Security Team

WebKit

Available for: macOS Tahoe

Impact: A malicious website may be able to process restricted web content outside the sandbox

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 308248

CVE-2026-28859: greenbynox, Arni Hardarson

WebKit Sandboxing

Available for: macOS Tahoe

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

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

WebKit Bugzilla: 306827

CVE-2026-20691: Gongyu Ma (@Mezone0)

Additional recognition

Accessibility

We would like to acknowledge Jacob Prezant (prezant.us) for their assistance.

Admin Framework

We would like to acknowledge Sota Toyokura for their assistance.

AirPort

We would like to acknowledge Frantisek Piekut, Yashar Shahinzadeh, Saman Ebrahimnezhad, Amir Safari, Omid Rezaii for their assistance.

Bluetooth

We would like to acknowledge Hamid Mahmoud for their assistance.

Captive Network

We would like to acknowledge Csaba Fitzl (@theevilbit) of Iru, Kun Peeks (@SwayZGl1tZyyy) for their assistance.

CipherML

We would like to acknowledge Nils Hanff (@nils1729@chaos.social) of Hasso Plattner Institute for their assistance.

CloudAttestation

We would like to acknowledge Suresh Sundaram, Willard Jansen for their assistance.

Core Bluetooth

We would like to acknowledge Nathaniel Oh (@calysteon) for their assistance.

CoreServices

We would like to acknowledge Fein, Iccccc & Ziiiro for their assistance.

CoreUI

We would like to acknowledge Peter Malone for their assistance.

Disk Images

We would like to acknowledge Jonathan Bar Or (@yo_yo_yo_jbo) for their assistance.

Find My

We would like to acknowledge Salemdomain for their assistance.

GPU Drivers

We would like to acknowledge Jian Lee (@speedyfriend433) for their assistance.

ICU

We would like to acknowledge Jian Lee (@speedyfriend433) for their assistance.

ImageKit

We would like to acknowledge Lyutoon and YenKoc, Mingxuan Yang (@PPPF00L), Minghao Lin (@Y1nKoc) and 风 (@binary_fmyy) of 抽象刷怪笼 for their assistance.

Kerberos v5 PAM module

We would like to acknowledge Jian Lee (@speedyfriend433) for their assistance.

Kernel

We would like to acknowledge DARKNAVY (@DarkNavyOrg), Kylian Boulard De Pouqueville From Fuzzinglabs, Patrick Ventuzelo From Fuzzinglabs, Robert Tran, Suresh Sundaram, Xinru Chi of Pangu Lab for their assistance.

libarchive

We would like to acknowledge Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs, Arni Hardarson for their assistance.

libc

We would like to acknowledge Vitaly Simonovich for their assistance.

Libnotify

We would like to acknowledge Ilias Morad (@A2nkF_) for their assistance.

LLVM

We would like to acknowledge Nathaniel Oh (@calysteon) for their assistance.

mDNSResponder

We would like to acknowledge William Mather for their assistance.

Messages

We would like to acknowledge JZ for their assistance.

MobileInstallation

We would like to acknowledge Gongyu Ma (@Mezone0) for their assistance.

Music

We would like to acknowledge Mohammad Kaif (@_mkahmad | kaif0x01) for their assistance.

Notes

We would like to acknowledge Dawuge of Shuffle Team and Hunan University for their assistance.

NSOpenPanel

We would like to acknowledge Barath Stalin K for their assistance.

ppp

We would like to acknowledge Dave G. for their assistance.

Quick Look

We would like to acknowledge Wojciech Regula of SecuRing (wojciechregula.blog), an anonymous researcher for their assistance.

Safari

We would like to acknowledge @RenwaX23, Farras Givari, Syarif Muhammad Sajjad, Yair for their assistance.

Sandbox

We would like to acknowledge Morris Richman (@morrisinlife), Prashan Samarathunge, 要乐奈 for their assistance.

Shortcuts

We would like to acknowledge Waleed Barakat (@WilDN00B) and Paul Montgomery (@nullevent) for their assistance.

Siri

We would like to acknowledge Anand Mallaya, Tech consultant, Anand Mallaya and Co., Harsh Kirdolia, Hrishikesh Parmar of Self-Employed, HvxyZLF, Kun Peeks (@SwayZGl1tZyyy) for their assistance.

Spotlight

We would like to acknowledge Bilge Kaan Mızrak, Claude & Friends: Risk Analytics Research Group, Zack Tickman for their assistance.

System Settings

We would like to acknowledge Christian Scalese (www.linkedin.com/in/christian-scalese-5794092aa), Karol Mazurek (@karmaz) of AFINE, Raffaele Sabato at SentinelOne for their assistance.

Time Zone

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) from Safran Mumbai India for their assistance.

UIKit

We would like to acknowledge AEC, Abhay Kailasia (@abhay_kailasia) from Safran Mumbai India, Bishal Kafle (@whoisbishal.k), Carlos Luna (U.S. Department of the Navy), Dalibor Milanovic, Daren Goodchild, JS De Mattei, Maxwell Garn, Zack Tickman, fuyuu12, incredincomp for their assistance.

Wallet

We would like to acknowledge Zhongcheng Li from IES Red Team of ByteDance for their assistance.

Web Extensions

We would like to acknowledge Carlos Jeurissen, Rob Wu (robwu.nl) for their assistance.

WebKit

We would like to acknowledge Vamshi Paili for their assistance.

Wi-Fi

We would like to acknowledge Kun Peeks (@SwayZGl1tZyyy), an anonymous researcher for their assistance.

Wi-Fi Connectivity

We would like to acknowledge Alex Radocea of Supernetworks, Inc for their assistance.

Widgets

We would like to acknowledge Marcel Voß, Mitul Pranjay, Serok Çelik for their assistance.

zsh

We would like to acknowledge Jian Lee (@speedyfriend433) for their assistance.

Published Date: March 24, 2026