About the security content of macOS Tahoe 26.2

This document describes the security content of macOS Tahoe 26.2.

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 26.2

Released December 12, 2025

App Store

Available for: macOS Tahoe

Impact: An app may be able to access sensitive payment tokens

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-46288: floeki, Zhongcheng Li from IES Red Team of ByteDance

AppleJPEG

Available for: macOS Tahoe

Impact: Processing a file may lead to memory corruption

Description: The issue was addressed with improved bounds checks.

CVE-2025-43539: Michael Reeves (@IntegralPilot)

AppleMobileFileIntegrity

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-2025-43523: an anonymous researcher

CVE-2025-43519: an anonymous researcher

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-2025-43522: an anonymous researcher

AppleMobileFileIntegrity

Available for: macOS Tahoe

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

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

CVE-2025-43521: an anonymous researcher

AppSandbox

Available for: macOS Tahoe

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

Description: A logic issue was addressed with improved file handling.

CVE-2025-46289: an anonymous researcher

AppSandbox

Available for: macOS Tahoe

Impact: An app may be able to access protected files within an App Sandbox container

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-46297: Mickey Jin (@patch1t)

Entry added January 9, 2026

Audio

Available for: macOS Tahoe

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

Description: The issue was addressed with improved input validation.

CVE-2025-43482: Jex Amro, Michael Reeves (@IntegralPilot)

Call History

Available for: macOS Tahoe

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

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

CVE-2025-43517: Wojciech Regula of SecuRing (wojciechregula.blog)

Calling Framework

Available for: macOS Tahoe

Impact: An attacker may be able to spoof their FaceTime caller ID

Description: An inconsistent user interface issue was addressed with improved state management.

CVE-2025-46287: an anonymous researcher, Riley Walz

CoreServices

Available for: macOS Tahoe

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

Description: A logic issue was addressed with improved validation.

CVE-2025-46283: an anonymous researcher

curl

Available for: macOS Tahoe

Impact: Multiple issues in curl

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-2024-7264

CVE-2025-9086

FaceTime

Available for: macOS Tahoe

Impact: Password fields may be unintentionally revealed when remotely controlling a device over FaceTime

Description: This issue was addressed with improved state management.

CVE-2025-43542: Yiğit Ocak

File Bookmark

Available for: macOS Tahoe

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

Description: A logic issue was addressed with improved checks.

CVE-2025-46281: an anonymous researcher

File Bookmark

Available for: macOS Tahoe

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

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

CVE-2025-43417: Ron Elemans

Entry added February 11, 2026

Foundation

Available for: macOS Tahoe

Impact: An app may be able to inappropriately access files through the spellcheck API

Description: A logic issue was addressed with improved checks.

CVE-2025-43518: Noah Gregory (wts.dev)

Foundation

Available for: macOS Tahoe

Impact: Processing malicious data may lead to unexpected app termination

Description: A memory corruption issue was addressed with improved bounds checking.

CVE-2025-43532: Andrew Calvano and Lucas Pinheiro of Meta Product Security

Game Center

Available for: macOS Tahoe

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

Description: The issue was addressed with improved handling of caches.

CVE-2025-46278: Kirin (@Pwnrin) and LFY (@secsys) of Fudan University

Icons

Available for: macOS Tahoe

Impact: An app may be able to identify what other apps a user has installed

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-46279: Duy Trần (@khanhduytran0)

Kernel

Available for: macOS Tahoe

Impact: An app may be able to elevate privileges

Description: A logic issue was addressed with improved checks.

CVE-2025-43512: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

Kernel

Available for: macOS Tahoe

Impact: An app may be able to gain root privileges

Description: An integer overflow was addressed by adopting 64-bit timestamps.

CVE-2025-46285: Kaitao Xie and Xiaolong Bai of Alibaba Group

LaunchServices

Available for: macOS Tahoe

Impact: An app may bypass Gatekeeper checks

Description: A logic issue was addressed with improved validation.

CVE-2025-46291: Kenneth Chew

libarchive

Available for: macOS Tahoe

Impact: Processing a file may lead to memory corruption

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-2025-5918

MDM Configuration Tools

Available for: macOS Tahoe

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

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

CVE-2025-43513: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

Messages

Available for: macOS Tahoe

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

Description: An information disclosure issue was addressed with improved privacy controls.

CVE-2025-46276: Rosyna Keller of Totally Not Malicious Software

Multi-Touch

Available for: macOS Tahoe

Impact: A malicious HID device may cause an unexpected process crash

Description: The issue was addressed with improved bounds checks.

CVE-2025-43533: Google Threat Analysis Group

CVE-2025-46300: Google Threat Analysis Group

CVE-2025-46301: Google Threat Analysis Group

CVE-2025-46302: Google Threat Analysis Group

CVE-2025-46303: Google Threat Analysis Group

CVE-2025-46304: Google Threat Analysis Group

CVE-2025-46305: Google Threat Analysis Group

Entry updated February 11, 2026

Networking

Available for: macOS Tahoe

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

Description: This issue was addressed with improved data protection.

CVE-2025-43509: Haoling Zhou, Shixuan Zhao (@NSKernel), Chao Wang (@evi0s), Zhiqiang Lin from SecLab of The Ohio State University

Notes

Available for: macOS Tahoe

Impact: An attacker with physical access may be able to view deleted notes

Description: The issue was addressed with improved handling of caches.

CVE-2025-43410: Atul R V

Photos

Available for: macOS Tahoe

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

Description: A configuration issue was addressed with additional restrictions.

CVE-2025-43428: an anonymous researcher, Michael Schmutzer of Technische Hochschule Ingolstadt

Safari

Available for: macOS Tahoe

Impact: On a Mac with Lockdown Mode enabled, web content opened via a file URL may be able to use Web APIs that should be restricted

Description: This issue was addressed with improved URL validation.

CVE-2025-43526: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

Safari Downloads

Available for: macOS Tahoe

Impact: A download's origin may be incorrectly associated

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-2024-8906: @retsew0x01

Screen Time

Available for: macOS Tahoe

Impact: An app may be able to access a user’s Safari history

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

CVE-2025-46277: Kirin (@Pwnrin)

Screen Time

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-2025-43538: Iván Savransky

Security

Available for: macOS Tahoe

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

Description: A logic issue was addressed with improved checks.

CVE-2025-46290: Bing Shi, Wenchao Li and Xiaolong Bai of Alibaba Group, and Luyi Xing of Indiana University Bloomington

Entry added February 11, 2026

Siri

Available for: macOS Tahoe

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

Description: The issue was addressed with improved handling of caches.

CVE-2025-43514: Morris Richman (@morrisinlife)

SoftwareUpdate

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-2025-43519: an anonymous researcher

StorageKit

Available for: macOS Tahoe

Impact: An app may be able to gain root privileges

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-43527: an anonymous researcher

sudo

Available for: macOS Tahoe

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

Description: A logic issue was addressed with improved restrictions.

CVE-2025-43416: Gergely Kalman (@gergely_kalman)

Voice Control

Available for: macOS Tahoe

Impact: A user with Voice Control enabled may be able to transcribe another user's activity

Description: A session management issue was addressed with improved checks.

CVE-2025-43516: Kay Belardinelli (Harvard University)

VoiceOver

Available for: macOS Tahoe

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

Description: This issue was addressed with improved checks.

CVE-2025-43530: Mickey Jin (@patch1t)

WebKit

Available for: macOS Tahoe

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

Description: The issue was addressed with additional permissions checks.

WebKit Bugzilla: 295941

CVE-2025-46282: Wojciech Regula of SecuRing (wojciechregula.blog)

WebKit

Available for: macOS Tahoe

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

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

WebKit Bugzilla: 301257

CVE-2025-43541: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

WebKit

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.

WebKit Bugzilla: 301726

CVE-2025-43536: Nan Wang (@eternalsakura13)

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: 300774

CVE-2025-43535: Google Big Sleep, Nan Wang (@eternalsakura13)

WebKit Bugzilla: 301468

CVE-2025-46298: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative, Nan Wang (@eternalsakura13)

Entry updated January 9, 2026

WebKit

Available for: macOS Tahoe

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

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

WebKit Bugzilla: 301371

CVE-2025-43501: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

WebKit

Available for: macOS Tahoe

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

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

WebKit Bugzilla: 301940

CVE-2025-43531: Phil Pizlo of Epic Games

WebKit

Available for: macOS Tahoe

Impact: Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 26. CVE-2025-14174 was also issued in response to this report.

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

WebKit Bugzilla: 302502

CVE-2025-43529: Google Threat Analysis Group

WebKit

Available for: macOS Tahoe

Impact: Processing maliciously crafted web content may lead to memory corruption. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 26. CVE-2025-43529 was also issued in response to this report.

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

WebKit Bugzilla: 303614

CVE-2025-14174: Apple and Google Threat Analysis Group

WebKit

Available for: macOS Tahoe

Impact: Processing maliciously crafted web content may disclose internal states of the app

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

WebKit Bugzilla: 299518

CVE-2025-46299: Google Big Sleep

Entry added January 9, 2026

WebKit Web Inspector

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.

WebKit Bugzilla: 300926

CVE-2025-43511: 이동하 (Lee Dong Ha of BoB 14th)

Additional recognition

AppleMobileFileIntegrity

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

Control Center

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

Core Services

We would like to acknowledge Golden Helm Securities, Csaba Fitzl (@theevilbit) of Iru and Gergely Kalman (@gergely_kalman) for their assistance.

Entry updated January 9, 2026

FileVault

We would like to acknowledge Nathaniel Oh (@calysteon) and Joel Peterson (@sekkyo) for their assistance.

Safari

We would like to acknowledge Mochammad Nosa Shandy Prastyo for their assistance.

Sandbox

We would like to acknowledge Arnaud Abbati for their assistance.

Voice Control

We would like to acknowledge PixiePoint Security for their assistance.

WebContentFilter

We would like to acknowledge Kun Peeks (@SwayZGl1tZyyy) for their assistance.

Entry added January 9, 2026

WebKit

We would like to acknowledge Geva Nurgandi Syahputra (gevakun) and Google Big Sleep for their assistance.

Entry updated January 9, 2026

Published Date: February 11, 2026