About the security content of tvOS 18.4

This document describes the security content of tvOS 18.4.

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.

tvOS 18.4

Released March 31, 2025

AirDrop

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An app may be able to read arbitrary file metadata

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24097: Ron Masas of BREAKPOINT.SH

AirPlay

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An attacker on the local network may be able to cause a denial-of-service

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

CVE-2025-31202: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without pairing

Description: An access issue was addressed with improved access restrictions.

CVE-2025-24271: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An attacker on the local network may be able to leak sensitive user information

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

CVE-2025-24270: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An attacker on the local network may be able to corrupt process memory

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

CVE-2025-24252: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An attacker on the local network may cause an unexpected app termination

Description: The issue was addressed with improved checks.

CVE-2025-24251: Uri Katz (Oligo Security)

CVE-2025-31197: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An attacker on the local network may be able to bypass authentication policy

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

CVE-2025-24206: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An attacker on the local network may cause an unexpected app termination

Description: A type confusion issue was addressed with improved checks.

CVE-2025-30445: Uri Katz (Oligo Security)

Entry added April 28, 2025

Audio

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: Processing a maliciously crafted font may result in the disclosure of process memory

Description: The issue was addressed with improved memory handling.

CVE-2025-24244: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

Audio

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: The issue was addressed with improved memory handling.

CVE-2025-24243: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

Calendar

Available for: Apple TV HD and Apple TV 4K (all models)

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

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

CVE-2025-30429: Denis Tokarev (@illusionofcha0s)

Calendar

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: This issue was addressed with improved checks.

CVE-2025-24212: Denis Tokarev (@illusionofcha0s)

CoreAudio

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: Parsing a file may lead to an unexpected app termination

Description: The issue was addressed with improved checks.

CVE-2025-24163: Google Threat Analysis Group

CoreAudio

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: Playing a malicious audio file may lead to an unexpected app termination

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

CVE-2025-24230: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreMedia

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: Processing a maliciously crafted video file may lead to unexpected app termination or corrupt process memory

Description: This issue was addressed with improved memory handling.

CVE-2025-24211: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreMedia

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: Processing a maliciously crafted video file may lead to unexpected app termination or corrupt process memory

Description: The issue was addressed with improved memory handling.

CVE-2025-24190: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreMedia Playback

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: A malicious app may be able to access private information

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

CVE-2025-30454: pattern-f (@pattern_F_)

CoreServices

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: This issue was addressed through improved state management.

CVE-2025-31191: Jonathan Bar Or (@yo_yo_yo_jbo) of Microsoft, and an anonymous researcher

CoreText

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: Processing a maliciously crafted font may result in the disclosure of process memory

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

CVE-2025-24182: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreUtils

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An attacker on the local network may be able to cause a denial-of-service

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

CVE-2025-31203: Uri Katz (Oligo Security)

Entry added April 28, 2025

curl

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An input validation issue was addressed

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-2024-9681

Foundation

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: The issue was resolved by sanitizing logging

CVE-2025-30447: LFY@secsys from Fudan University

ImageIO

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: Parsing an image may lead to disclosure of user information

Description: A logic error was addressed with improved error handling.

CVE-2025-24210: Anonymous working with Trend Micro Zero Day Initiative

Kernel

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: A malicious app may be able to attempt passcode entries on a locked device and thereby cause escalating time delays after 4 failures

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

CVE-2025-30432: Michael (Biscuit) Thomas - @biscuit@social.lol

libarchive

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An input validation issue was addressed

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-2024-48958

libnetcore

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: Processing maliciously crafted web content may result in the disclosure of process memory

Description: A logic issue was addressed with improved checks.

CVE-2025-24194: an anonymous researcher

libxml2

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: Parsing a file may lead to an 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-2025-27113

CVE-2024-56171

libxpc

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: This issue was addressed through improved state management.

CVE-2025-24178: an anonymous researcher

libxpc

Available for: Apple TV HD and Apple TV 4K (all models)

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

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

CVE-2025-31182: Alex Radocea and Dave G. of Supernetworks, 风沐云烟(@binary_fmyy) and Minghao Lin(@Y1nKoc)

libxpc

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: An app may be able to gain elevated privileges

Description: A logic issue was addressed with improved checks.

CVE-2025-24238: an anonymous researcher

NetworkExtension

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: This issue was addressed with additional entitlement checks.

CVE-2025-30426: Jimmy

Power Services

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: This issue was addressed with additional entitlement checks.

CVE-2025-24173: Mickey Jin (@patch1t)

Security

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: A validation issue was addressed with improved logic.

CVE-2025-30471: Bing Shi, Wenchao Li, Xiaolong Bai of Alibaba Group, Luyi Xing of Indiana University Bloomington

Share Sheet

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: A malicious app may be able to dismiss the system notification on the Lock Screen that a recording was started

Description: This issue was addressed with improved access restrictions.

CVE-2025-30438: Halle Winkler, Politepix theoffcuts.org

Siri

Available for: Apple TV HD and Apple TV 4K (all models)

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

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

CVE-2025-31183: Kirin (@Pwnrin), Bohdan Stasiuk (@bohdan_stasiuk)

Siri

Available for: Apple TV HD and Apple TV 4K (all models)

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

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

CVE-2025-24217: Kirin (@Pwnrin)

Siri

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: A privacy issue was addressed by not logging contents of text fields.

CVE-2025-24214: Kirin (@Pwnrin)

WebKit

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 285892

CVE-2025-24264: Gary Kwong, and an anonymous researcher

WebKit Bugzilla: 284055

CVE-2025-24216: Paul Bakker of ParagonERP

WebKit

Available for: Apple TV HD and Apple TV 4K (all models)

Impact: A type confusion issue could lead to memory corruption

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

WebKit Bugzilla: 286694

CVE-2025-24213: Google V8 Security Team

WebKit

Available for: Apple TV HD and Apple TV 4K (all models)

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: 286462

CVE-2025-24209: Francisco Alonso (@revskills), and an anonymous researcher

WebKit

Available for: Apple TV HD and Apple TV 4K (all models)

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

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

WebKit Bugzilla: 285643

CVE-2025-30427: rheza (@ginggilBesel)

WebKit

Available for: Apple TV HD and Apple TV 4K (all models)

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

Description: This issue was addressed through improved state management.

WebKit Bugzilla: 286580

CVE-2025-30425: an anonymous researcher

Additional recognition

Accounts

We would like to acknowledge Bohdan Stasiuk (@bohdan_stasiuk) for their assistance.

AirPlay

We would like to acknowledge Uri Katz (Oligo Security) for their assistance.

Entry added April 28, 2025

Apple Account

We would like to acknowledge Byron Fecho for their assistance.

Audio

We would like to acknowledge Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative for their assistance.

Find My

We would like to acknowledge 神罚(@Pwnrin) for their assistance.

Foundation

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

Handoff

We would like to acknowledge Kirin and FlowerCode for their assistance.

HearingCore

We would like to acknowledge Kirin@Pwnrin and LFY@secsys from Fudan University for their assistance.

ImageIO

We would like to acknowledge D4m0n for their assistance.

Photos

We would like to acknowledge Bistrit Dahal for their assistance.

Sandbox Profiles

We would like to acknowledge Benjamin Hornbeck for their assistance.

SceneKit

We would like to acknowledge Marc Schoenefeld, Dr. rer. nat. for their assistance.

Security

We would like to acknowledge Kevin Jones (GitHub) for their assistance.

Siri

We would like to acknowledge Lyutoon for their assistance.

WebKit

We would like to acknowledge Gary Kwong, P1umer (@p1umer) and Q1IQ (@q1iqF), Wai Kin Wong, Dongwei Xiao, Shuai Wang and Daoyuan Wu of HKUST Cybersecurity Lab, Anthony Lai(@darkfloyd1014) of VXRL, Wong Wai Kin, Dongwei Xiao and Shuai Wang of HKUST Cybersecurity Lab, Anthony Lai (@darkfloyd1014) of VXRL., Xiangwei Zhang of Tencent Security YUNDING LAB, 냥냥, and an anonymous researcher for their assistance.

Published Date: April 30, 2025