

# About the security content of tvOS 26.2

This document describes the security content of tvOS 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.

## tvOS 26.2

Released December 12, 2025

### AppleJPEG

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

Impact: Processing a file may lead to memory corruption

Description: The issue was addressed with improved bounds checks.

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

### curl

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

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](https://cve.org).

CVE-2024-7264

CVE-2025-9086

### Foundation

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

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

### Icons

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

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

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

## Multi-Touch

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

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

## 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 race condition was addressed with improved state handling.

WebKit Bugzilla: 301940

CVE-2025-43531: Phil Pizlo of Epic Games

## WebKit

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

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

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

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

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: The issue was addressed with improved memory handling.

WebKit Bugzilla: 301468

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

Entry added January 9, 2026

## Additional recognition

### AppleMobileFileIntegrity

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

# WebKit

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

Entry updated January 9, 2026


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: February 11, 2026

Helpful?

Yes

No

 > Support > About the security content of tvOS 26.2

Copyright © 2026 Apple Inc. All rights reserved.

[Privacy Policy](#)

[Terms of Use](#)

[Sales and Refunds](#)

[Site Map](#)

United States