About the security content of iPadOS 17.7.6

This document describes the security content of iPadOS 17.7.6.

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.

iPadOS 17.7.6

Released March 31, 2025

Accounts

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

Impact: Sensitive keychain data may be accessible from an iOS backup

Description: This issue was addressed with improved data access restriction.

CVE-2025-24221: Lehan Dilusha @zorrosign Sri Lanka, and an anonymous researcher

Audio

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Audio

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

BiometricKit

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Description: A buffer overflow was addressed with improved bounds checking.

CVE-2025-24237: Yutong Xiu

Calendar

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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)

CloudKit

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Description: The issue was addressed with improved checks.

CVE-2025-24215: Kirin (@Pwnrin)

CoreAudio

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

Impact: A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2.

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

CVE-2025-24085

CoreMedia

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

curl

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Kernel

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Description: The issue was addressed with improved checks.

CVE-2025-24203: Ian Beer of Google Project Zero

libxml2

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

NetworkExtension

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Photos

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Description: This issue was addressed through improved state management.

CVE-2025-30428: Jax Reissner

Power Services

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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)

Safari

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

Impact: Visiting a malicious website may lead to user interface spoofing

Description: The issue was addressed with improved UI.

CVE-2025-24113: @RenwaX23

Security

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Shortcuts

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

Impact: A shortcut may be able to access files that are normally inaccessible to the Shortcuts app

Description: A permissions issue was addressed with improved validation.

CVE-2025-30465: an anonymous researcher

Shortcuts

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

Impact: A shortcut may be able to access files that are normally inaccessible to the Shortcuts app

Description: This issue was addressed with improved access restrictions.

CVE-2025-30433: Andrew James Gonzalez

Siri

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

Impact: An attacker with physical access may be able to use Siri to access sensitive user data

Description: This issue was addressed by restricting options offered on a locked device.

CVE-2025-24198: Richard Hyunho Im (@richeeta) with routezero.security

Siri

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

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

CVE-2025-24205: YingQi Shi(@Mas0nShi) of DBAppSecurity's WeBin lab and Minghao Lin (@Y1nKoc)

WebKit

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

Impact: Maliciously crafted web content may be able to break out of Web Content sandbox. This is a supplementary fix for an attack that was blocked in iOS 17.2. (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 17.2.)

Description: An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions.

WebKit Bugzilla: 285858

CVE-2025-24201: Apple

Entry Added April 9, 2025

WebKit

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

WebKit

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 284055

CVE-2025-24216: Paul Bakker of ParagonERP

WebKit Bugzilla: 285892

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

WebKit

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

Impact: Processing maliciously crafted web content may lead to memory corruption

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 282450

CVE-2024-54543: Lukas Bernhard, Gary Kwong, and an anonymous researcher

WebKit Bugzilla: 277967

CVE-2024-54534: Tashita Software Security

WebKit

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 282180

CVE-2024-54508: Xiangwei Zhang of Tencent Security YUNDING LAB, linjy of HKUS3Lab and chluo of WHUSecLab, and an anonymous researcher

WebKit

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Description: The issue was addressed with improved checks.

WebKit Bugzilla: 281912

CVE-2024-54502: Brendon Tiszka of Google Project Zero

WebKit

Available for: iPad Pro 12.9-inch 2nd generation, iPad Pro 10.5-inch, and iPad 6th generation

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

Additional recognition

Audio

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

Security

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

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: April 10, 2025

Helpful? Yes No