About the security content of iPadOS 17.7.7

This document describes the security content of iPadOS 17.7.7.

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 17.7.7

Released May 12, 2025

AirDrop

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 read arbitrary file metadata

Description: A permissions issue was addressed with additional restrictions.

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

AppleJPEG

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

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

Description: The issue was addressed with improved input sanitization.

CVE-2025-31251: 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: An app may be able to cause unexpected system termination

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

CVE-2025-31235: Dillon Franke working with Google Project Zero

CoreAudio

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: The issue was addressed with improved checks.

CVE-2025-31208: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreGraphics

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 a denial-of-service or potentially disclose memory contents

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

CVE-2025-31196: wac working with Trend Micro Zero Day Initiative

CoreGraphics

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 disclosure of user information

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

CVE-2025-31209: 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: Parsing a file may lead to an unexpected app termination

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

CVE-2025-31239: 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: The issue was addressed with improved input sanitization.

CVE-2025-31233: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

Display

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 memory corruption issue was addressed with improved state management.

CVE-2025-24111: Wang Yu of Cyberserval

FaceTime

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

Impact: Processing web content may lead to a denial-of-service

Description: The issue was addressed with improved UI.

CVE-2025-31210: Andrew James Gonzalez

iCloud Document Sharing

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

Impact: An attacker may be able to turn on sharing of an iCloud folder without authentication

Description: This issue was addressed with additional entitlement checks.

CVE-2025-30448: Lyutoon and YenKoc, Dayton Pidhirney of Atredis Partners

ImageIO

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

Impact: Processing a maliciously crafted image may lead to a denial-of-service

Description: A logic issue was addressed with improved checks.

CVE-2025-31226: Saagar Jha

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 leak sensitive kernel state

Description: An information disclosure issue was addressed by removing the vulnerable code.

CVE-2025-24144: Mateusz Krzywicki (@krzywix)

Kernel

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

Impact: An attacker may be able to cause unexpected system termination or corrupt kernel memory

Description: The issue was addressed with improved memory handling.

CVE-2025-31219: Michael DePlante (@izobashi) and Lucas Leong (@_wmliang_) of 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 remote attacker may cause an unexpected app termination

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

CVE-2025-31241: Christian Kohlschütter

libexpat

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

Impact: Multiple issues in libexpat, including unexpected app termination or arbitrary code execution

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-2024-8176

Mail Addressing

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

Impact: Processing an email may lead to user interface spoofing

Description: An injection issue was addressed with improved input validation.

CVE-2025-24225: Richard Hyunho Im (@richeeta)

Notes

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

Impact: An attacker with physical access to a device may be able to access notes from the lock screen

Description: The issue was addressed with improved authentication.

CVE-2025-31228: Andr.Ess

Parental Controls

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 retrieve Safari bookmarks without an entitlement check

Description: This issue was addressed with additional entitlement checks.

CVE-2025-24259: Noah Gregory (wts.dev)

Pro Res

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: The issue was addressed with improved checks.

CVE-2025-31245: wac

Sandbox Profiles

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 read a persistent device identifier

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24220: Wojciech Regula of SecuRing (wojciechregula.blog)

Security

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

Impact: A remote attacker may be able to leak memory

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

CVE-2025-31221: Dave G.

Security

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 associated usernames and websites in a user's iCloud Keychain

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

CVE-2025-31213: Kirin (@Pwnrin) and 7feilee

StoreKit

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

CVE-2025-31242: Eric Dorphy of Twin Cities App Dev LLC

Weather

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 read sensitive location information

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

CVE-2025-31220: Adam M.

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

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 input validation.

WebKit Bugzilla: 289677

CVE-2025-31217: Ignacio Sanmillan (@ulexec)

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: 288814

CVE-2025-31215: Jiming Wang and Jikai Ren

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 type confusion issue was addressed with improved state handling.

WebKit Bugzilla: 290834

CVE-2025-31206: an anonymous researcher

Additional recognition

Kernel

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

Published Date: May 12, 2025