About the security content of iPadOS 17.7.9

This document describes the security content of iPadOS 17.7.9.

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 17.7.9

Released July 29, 2025

Accessibility

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

Impact: Privacy Indicators for microphone or camera access may not be correctly displayed

Description: The issue was addressed by adding additional logic.

CVE-2025-43217: Himanshu Bharti (@Xpl0itme)

CFNetwork

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 app termination

Description: A use-after-free issue was addressed by removing the vulnerable code.

CVE-2025-43222: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

CFNetwork

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

Impact: A non-privileged user may be able to modify restricted network settings

Description: A denial-of-service issue was addressed with improved input validation.

CVE-2025-43223: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

copyfile

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 protected user data

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

CVE-2025-43220: Mickey Jin (@patch1t)

CoreMedia

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: An out-of-bounds access issue was addressed with improved bounds checking.

CVE-2025-43210: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreMedia Playback

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: The issue was addressed with additional permissions checks.

CVE-2025-43230: Chi Yuan Chang of ZUSO ART and taikosoup

Find My

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 fingerprint the user

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-31279: Dawuge of Shuffle Team

ICU

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: An out-of-bounds access issue was addressed with improved bounds checking.

CVE-2025-43209: Gary Kwong working with Trend Micro Zero Day Initiative

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 result in disclosure of process memory

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

CVE-2025-43226

Kernel

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 cause unexpected system termination

Description: The issue was addressed with improved checks.

CVE-2025-24224: Tony Iskow (@Tybbow)

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 cause unexpected system termination

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

CVE-2025-43282: Christian Kohlschütter

Entry added October 15, 2025

libxslt

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: 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-2025-7424: Ivan Fratric of Google Project Zero

Mail Drafts

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

Impact: Remote content may be loaded even when the 'Load Remote Images' setting is turned off

Description: This issue was addressed through improved state management.

CVE-2025-31276: Himanshu Bharti (@Xpl0itme)

Notes

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 logging issue was addressed with improved data redaction.

CVE-2025-43225: Kirin (@Pwnrin)

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)

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: 291742

CVE-2025-31278: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

WebKit

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 memory handling.

WebKit Bugzilla: 293730

CVE-2025-43211: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

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: 295382

CVE-2025-43216: 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 Safari crash

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.

WebKit Bugzilla: 296459

CVE-2025-6558: Clément Lecigne and Vlad Stolyarov of Google's Threat Analysis Group

Additional recognition

CoreAudio

We would like to acknowledge @zlluny, Noah Weinberg for their assistance.

Device Management

We would like to acknowledge Al Karak for their assistance.

Game Center

We would like to acknowledge YingQi Shi (@Mas0nShi) of DBAppSecurity's WeBin lab for their assistance.

libxml2

We would like to acknowledge Sergei Glazunov of Google Project Zero for their assistance.

libxslt

We would like to acknowledge Ivan Fratric of Google Project Zero for their assistance.

Shortcuts

We would like to acknowledge Chi Yuan Chang of ZUSO ART and taikosoup, and Dennis Kniep for their assistance.

Published Date: October 15, 2025