About the security content of iOS 18.5 and iPadOS 18.5

This document describes the security content of iOS 18.5 and iPadOS 18.5.

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.

iOS 18.5 and iPadOS 18.5

Released May 12, 2025

AppleJPEG

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Baseband

Available for: iPhone 16e

Impact: An attacker in a privileged network position may be able to intercept network traffic

Description: This issue was addressed through improved state management.

CVE-2025-31214: 秦若涵, 崔志伟, and 崔宝江

Call History

Available for: iPhone XS and later

Impact: Call history from deleted apps may still appear in spotlight search results

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

CVE-2025-31225: Deval Jariwala

Core Bluetooth

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: This issue was addressed through improved state management.

CVE-2025-31212: Guilherme Rambo of Best Buddy Apps (rambo.codes)

CoreAudio

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

FaceTime

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: Muting the microphone during a FaceTime call may not result in audio being silenced

Description: This issue was addressed through improved state management.

CVE-2025-31253: Dalibor Milanovic

FaceTime

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

FrontBoard

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: A logic issue was addressed with improved checks.

CVE-2025-31207: YingQi Shi (@Mas0nShi) of DBAppSecurity's WeBin lab, Duy Trần (@khanhduytran0)

iCloud Document Sharing

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: Dayton Pidhirney of Atredis Partners, Lyutoon and YenKoc

ImageIO

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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)

mDNSResponder

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: A user may be able to elevate privileges

Description: A correctness issue was addressed with improved checks.

CVE-2025-31222: Paweł Płatek (Trail of Bits)

Notes

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Notes

Available for: iPhone XS and later

Impact: An attacker with physical access to a device may be able to access a deleted call recording

Description: A logic issue was addressed with improved checks.

CVE-2025-31227: Shehab Khan

Pro Res

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: The issue was addressed with improved checks.

CVE-2025-31245: wac

Pro Res

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: The issue was addressed with improved input sanitization.

CVE-2025-31234: CertiK (@CertiK)

Security

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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.

WebKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: The issue was addressed with improved checks.

WebKit Bugzilla: 289387

CVE-2025-31223: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

WebKit Bugzilla: 289653

CVE-2025-31238: wac working with Trend Micro Zero Day Initiative

WebKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 287577

CVE-2025-24223: rheza (@ginggilBesel) and an anonymous researcher

WebKit Bugzilla: 291506

CVE-2025-31204: Nan Wang(@eternalsakura13)

WebKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

WebKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: A malicious website may exfiltrate data cross-origin

Description: The issue was addressed with improved checks.

WebKit Bugzilla: 290992

CVE-2025-31205: Ivan Fratric of Google Project Zero

WebKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th

generation and later, and iPad mini 5th generation and later

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

Description: This issue was addressed with improved memory handling.

WebKit Bugzilla: 290985

CVE-2025-31257: Juergen Schmied of Lynck GmbH

Additional recognition

AirDrop

We would like to acknowledge Dalibor Milanovic for their assistance.

Kernel

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

libnetcore

We would like to acknowledge Hoffcona of ByteDance IES Red Team for their assistance.

Messages

We would like to acknowledge Paulo Henrique Batista Rosa de Castro (@paulohbrc) for their assistance.

MobileGestalt

We would like to acknowledge iisBuri for their assistance.

MobileLockdown

We would like to acknowledge Matthias Frielingsdorf (@helthydriver) of iVerify, an anonymous researcher for their assistance.

NetworkExtension

We would like to acknowledge Andrei-Alexandru Bleorțu for their assistance.

Phone

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) from C-DAC Thiruvananthapuram India for their assistance.

Photos

We would like to acknowledge Yusuf Kelany for their assistance.

Safari

We would like to acknowledge Akash Labade, Narendra Bhati, Manager of Cyber Security at Suma Soft Pvt. Ltd, Pune (India) for their assistance.

Screenshots

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

Shortcuts

We would like to acknowledge Candace Jensen of Kandji, Chi Yuan Chang of ZUSO ART and taikosoup, Egor Filatov (Positive Technologies), Monnier Pascaud for their assistance.

Siri Suggestions

We would like to acknowledge Jake Derouin (jakederouin.com) for their assistance.

Spotlight

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) from C-DAC Thiruvananthapuram India for their assistance.

WebKit

We would like to acknowledge Mike Dougherty and Daniel White of Google Chrome and an anonymous researcher for their assistance.

Published Date: May 12, 2025