About the security content of iOS 18.7.5 and iPadOS 18.7.5

This document describes the security content of iOS 18.7.5 and iPadOS 18.7.5.

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 18.7.5 and iPadOS 18.7.5

Released February 11, 2026

Accessibility

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: An attacker with physical access to a locked device may be able to view sensitive user information

Description: An inconsistent user interface issue was addressed with improved state management.

CVE-2026-20645: Wong Wee Xiang and Loh Boon Keat

Entry updated March 24, 2026

Books

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: Restoring a maliciously crafted backup file may lead to modification of protected system files

Description: A path handling issue was addressed with improved validation.

CVE-2025-43537: piffz, Daniel Nurkin, Al Sadman Awal, Mohamed Hamdadou & Mahran Alhazmi, Hichem Maloufi, Christian Mina, Gerson Aldaz, qwerty j0y & Ricardo Garcia, Dorian Del Valle

Entry updated March 24, 2026

CFNetwork

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: A remote user may be able to write arbitrary files

Description: A path handling issue was addressed with improved logic.

CVE-2026-20660: Amy (amys.website)

CoreAudio

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th 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-2026-20611: Anonymous working with Trend Micro Zero Day Initiative

CoreMedia

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: Processing a maliciously crafted file may lead to a denial-of-service or potentially disclose memory contents

Description: The issue was addressed with improved memory handling.

CVE-2026-20609: Yiğit Can YILMAZ (@yilmazcanyigit)

ImageIO

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: Processing a maliciously crafted image may result in disclosure of process memory

Description: The issue was addressed with improved memory handling.

CVE-2026-20634: George Karchemsky (@gkarchemsky) working with Trend Micro Zero Day Initiative

ImageIO

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: Processing a maliciously crafted image may lead to disclosure of user information

Description: The issue was addressed with improved bounds checks.

CVE-2026-20675: George Karchemsky (@gkarchemsky) working with Trend Micro Zero Day Initiative

Kernel

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

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

Description: A logic issue was addressed with improved checks.

CVE-2026-20671: Xin'an Zhou, Juefei Pu, Zhutian Liu, Zhiyun Qian, Zhaowei Tan, Srikanth V. Krishnamurthy, Mathy Vanhoef

LaunchServices

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

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

Description: The issue was resolved by sanitizing logging.

CVE-2026-20663: Zhongcheng Li from IES Red Team

libexpat

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

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

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-2025-59375

libnetcore

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

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

Description: A logic issue was addressed with improved checks.

CVE-2026-20671: Xin'an Zhou, Juefei Pu, Zhutian Liu, Zhiyun Qian, Zhaowei Tan, Srikanth V. Krishnamurthy, Mathy Vanhoef

Live Captions

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: An attacker with physical access to a locked device may be able to view sensitive user information

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

CVE-2026-20655: Richard Hyunho Im (@richeeta) at Route Zero Security (routezero.security)

Mail

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: Turning off "Load remote content in messages" may not apply to all mail previews

Description: A logic issue was addressed with improved checks.

CVE-2026-20673: an anonymous researcher

Messages

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: A shortcut may be able to bypass sandbox restrictions

Description: A race condition was addressed with improved handling of symbolic links.

CVE-2026-20677: Ron Masas of BreakPoint.SH

Model I/O

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: Processing a maliciously crafted USD file may lead to unexpected app termination

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

CVE-2026-20616: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Multi-Touch

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

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

Safari

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: An app may be able to access a user's Safari history

Description: A logic issue was addressed with improved validation.

CVE-2026-20656: Mickey Jin (@patch1t)

Sandbox

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: An app may be able to break out of its sandbox

Description: A permissions issue was addressed with additional restrictions.

CVE-2026-20628: Noah Gregory (wts.dev)

Sandbox Profiles

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

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

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

CVE-2026-20678: Óscar García Pérez, Stanislav Jelezoglo

Screenshots

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: An attacker may be able to discover a user's deleted notes

Description: A logic issue was addressed with improved state management.

CVE-2026-20682: Viktor Lord Härringtón

Shortcuts

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

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

Description: A parsing issue in the handling of directory paths was addressed with improved path validation.

CVE-2026-20653: Enis Maholli (enismaholli.com)

Spotlight

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: A sandboxed app may be able to access sensitive user data

Description: The issue was addressed with additional restrictions on the observability of app states.

CVE-2026-20680: an anonymous researcher

StoreKit

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: An app may be able to identify what other apps a user has installed

Description: A privacy issue was addressed with improved checks.

CVE-2026-20641: Gongyu Ma (@Mezone0)

UIKit

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: An app may be able to bypass certain Privacy preferences

Description: This issue was addressed by removing the vulnerable code.

CVE-2026-20606: LeminLimez

Voice Control

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: An app may be able to crash a system process

Description: The issue was addressed with improved memory handling.

CVE-2026-20605: @cloudlldb of @pixiepointsec

VoiceOver

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: An attacker with physical access to a locked device may be able to view sensitive user information

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

CVE-2026-20661: Dalibor Milanovic

WebKit

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

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

Description: This issue was addressed through improved state management.

WebKit Bugzilla: 303357

CVE-2026-20608: HanQing from TSDubhe and Nan Wang (@eternalsakura13)

WebKit

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

Impact: A remote attacker may be able to cause a denial-of-service

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 303959

CVE-2026-20652: Nathaniel Oh (@calysteon)

WebKit

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th 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: 303444

CVE-2026-20644: HanQing from TSDubhe and Nan Wang (@eternalsakura13)

WebKit Bugzilla: 304661

CVE-2026-20635: EntryHi

Wi-Fi

Available for: iPhone XS, iPhone XS Max, iPhone XR, iPad 7th generation

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

Description: The issue was addressed with improved memory handling.

CVE-2026-20621: Wang Yu of Cyberserval

Additional recognition

ImageIO

We would like to acknowledge George Karchemsky (@gkarchemsky) working with Trend Micro Zero Day Initiative for their assistance.

Kernel

We would like to acknowledge Xinru Chi of Pangu Lab for their assistance.

libpthread

We would like to acknowledge Fabiano Anemone for their assistance.

WebKit

We would like to acknowledge EntryHi, Stanislav Fort of Aisle Research, Vsevolod Kokorin (Slonser) of Solidlab and Jorian Woltjer for their assistance.

Published Date: March 24, 2026