About the security content of iOS 16.7.6 and iPadOS 16.7.6

This document describes the security content of iOS 16.7.6 and iPadOS 16.7.6.

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.

iOS 16.7.6 and iPadOS 16.7.6

Released March 5, 2024

Accessibility

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: An app may be able to spoof system notifications and UI

Description: This issue was addressed with additional entitlement checks.

CVE-2024-23262: Guilherme Rambo of Best Buddy Apps (rambo.codes)

Entry added March 7, 2024

CoreCrypto

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: An attacker may be able to decrypt legacy RSA PKCS#1 v1.5 ciphertexts without having the private key

Description: A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions.

CVE-2024-23218: Clemens Lang

Entry added March 7, 2024

ImageIO

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: Processing an image may lead to arbitrary code execution

Description: A buffer overflow issue was addressed with improved memory handling.

CVE-2024-23286: Junsung Lee working with Trend Micro Zero Day Initiative, Amir Bazine and Karsten König of CrowdStrike Counter Adversary Operations, Dohyun Lee (@l33d0hyun), and Lyutoon and Mr.R

Entry added March 7, 2024, updated May 29, 2024

ImageIO

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: Processing an image may result in disclosure of process memory

Description: The issue was addressed with improved memory handling.

CVE-2024-23257: Junsung Lee working with Trend Micro Zero Day Initiative

Entry added March 7, 2024

Kernel

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited.

Description: A memory corruption issue was addressed with improved validation.

CVE-2024-23225

Kernel

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

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

Description: A race condition was addressed with additional validation.

CVE-2024-23235

Entry added March 7, 2024

Kernel

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

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

Description: A memory corruption vulnerability was addressed with improved locking.

CVE-2024-23265: Xinru Chi of Pangu Lab

Entry added March 7, 2024

libxpc

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

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

Description: The issue was addressed with improved checks.

CVE-2024-23278: an anonymous researcher

Entry added March 7, 2024

MediaRemote

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

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

Description: This issue was addressed with improved redaction of sensitive information.

CVE-2023-28826: Meng Zhang (鲸落) of NorthSea

Entry added March 7, 2024

Metal

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: An application may be able to read restricted memory

Description: A validation issue was addressed with improved input sanitization.

CVE-2024-23264: Meysam Firouzi @R00tkitsmm working with Trend Micro Zero Day Initiative

Entry added March 7, 2024

Notes

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

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

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

CVE-2024-23283

Entry added March 7, 2024

Safari

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

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

Description: The issue was addressed with improved checks.

CVE-2024-23259: Lyra Rebane (rebane2001)

Entry added March 7, 2024

Share Sheet

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

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

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

CVE-2024-23231: Kirin (@Pwnrin) and luckyu (@uuulucky)

Entry added March 7, 2024

Shortcuts

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: A shortcut may be able to use sensitive data with certain actions without prompting the user

Description: The issue was addressed with additional permissions checks.

CVE-2024-23204: Jubaer Alnazi (@h33tjubaer)

CVE-2024-23203: an anonymous researcher

Entry added March 7, 2024

Siri

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: A person with physical access to a device may be able to use Siri to access private calendar information

Description: A lock screen issue was addressed with improved state management.

CVE-2024-23289: Lewis Hardy

Entry added March 7, 2024

UIKit

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

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

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

CVE-2024-23246: Deutsche Telekom Security GmbH sponsored by Bundesamt für Sicherheit in der Informationstechnik

Entry added March 7, 2024

WebKit

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: Processing maliciously crafted web content may prevent Content Security Policy from being enforced

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

WebKit Bugzilla: 267241

CVE-2024-23284: Georg Felber and Marco Squarcina

Entry added March 7, 2024

WebKit

Available for: iPhone 8, iPhone 8 Plus, iPhone X, iPad 5th generation, iPad Pro 9.7-inch, and iPad Pro 12.9-inch 1st generation

Impact: Processing maliciously crafted web content may prevent Content Security Policy from being enforced

Description: A logic issue was addressed with improved validation.

WebKit Bugzilla: 264811

CVE-2024-23263: Johan Carlsson (joaxcar)

Entry added March 7, 2024

Additional recognition

Messages

We would like to acknowledge Petar Mataić for their assistance.

Entry added February 5, 2025

Published Date: February 05, 2025