About the security content of iOS 17.4 and iPadOS 17.4

This document describes the security content of iOS 17.4 and iPadOS 17.4.

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 17.4 and iPadOS 17.4

Released March 5, 2024

Accessibility

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to read sensitive location information

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

CVE-2024-23243: Cristian Dinca of "Tudor Vianu" National High School of Computer Science, Romania

Accessibility

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

Accessibility

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: A malicious app may be able to observe user data in log entries related to accessibility notifications

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

CVE-2024-23291

Entry added March 7, 2024

AppleMobileFileIntegrity

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to elevate privileges

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

CVE-2024-23288: Wojciech Regula of SecuRing (wojciechregula.blog) and Kirin (@Pwnrin)

Entry added March 7, 2024

Bluetooth

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An attacker in a privileged network position may be able to inject keystrokes by spoofing a keyboard

Description: The issue was addressed with improved checks.

CVE-2024-23277: Marc Newlin of SkySafe

Entry added March 7, 2024

CoreBluetooth - LE

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to access Bluetooth-connected microphones without user permission

Description: An access issue was addressed with improved access restrictions.

CVE-2024-23250: Guilherme Rambo of Best Buddy Apps (rambo.codes)

Entry added March 7, 2024

ExtensionKit

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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-2024-23205

Entry added March 7, 2024

file

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

Description: This issue was addressed with improved checks.

CVE-2022-48554

Entry added March 7, 2024

Image Processing

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to execute arbitrary code with kernel privileges

Description: The issue was addressed with improved memory handling.

CVE-2024-23270: an anonymous researcher

Entry added March 7, 2024

ImageIO

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

Kernel

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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 XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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 XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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 XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

libxpc

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges

Description: The issue was addressed with improved memory handling.

CVE-2024-0258: ali yabuz

Entry added March 7, 2024

MediaRemote

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: A malicious application may be able to access private information

Description: The issue was addressed with improved checks.

CVE-2024-23297: scj643

Entry added March 7, 2024

Messages

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

Description: A privacy issue was addressed with improved handling of temporary files.

CVE-2024-23287: Kirin (@Pwnrin)

Entry added March 7, 2024

Metal

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

Photos

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: Shake-to-undo may allow a deleted photo to be re-surfaced without authentication

Description: The issue was addressed with improved checks.

CVE-2024-23240: Harsh Tyagi

Entry added March 7, 2024

Photos

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: Photos in the Hidden Photos Album may be viewed without authentication

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

CVE-2024-23255: Harsh Tyagi

Entry added March 7, 2024

RTKit

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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-2024-23296

Safari

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to fingerprint the user

Description: The issue was addressed with improved handling of caches.

CVE-2024-23220

Entry added March 7, 2024

Safari

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th 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 checks.

CVE-2024-23259: Lyra Rebane (rebane2001)

Entry added March 7, 2024

Safari Private Browsing

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: A user's locked tabs may be briefly visible while switching tab groups when Locked Private Browsing is enabled

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

CVE-2024-23256: Om Kothawade

Safari Private Browsing

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: Private Browsing tabs may be accessed without authentication

Description: This issue was addressed through improved state management.

CVE-2024-23273: Matej Rabzelj

Entry added March 7, 2024

Sandbox

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to leak sensitive user information

Description: A race condition was addressed with improved state handling.

CVE-2024-23239: Mickey Jin (@patch1t)

Entry added March 7, 2024

Sandbox

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

Description: A logic issue was addressed with improved restrictions.

CVE-2024-23290: Wojciech Regula of SecuRing (wojciechregula.blog)

Entry added March 7, 2024

Share Sheet

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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 XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to access information about a user's contacts

Description: This issue was addressed with improved data protection.

CVE-2024-23292: K宝 and LFY@secsys from Fudan University

Entry added March 7, 2024

Siri

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

Siri

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An attacker with physical access may be able to use Siri to access sensitive user data

Description: This issue was addressed through improved state management.

CVE-2024-23293: Bistrit Dahal

Entry added March 7, 2024

Spotlight

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to leak sensitive user information

Description: This issue was addressed through improved state management.

CVE-2024-23241

Entry added March 7, 2024

Synapse

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to view Mail data

Description: A privacy issue was addressed by not logging contents of text fields.

CVE-2024-23242

Entry added March 7, 2024

UIKit

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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 XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th 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 memory handling.

WebKit Bugzilla: 263758

CVE-2024-54658: anbu1024 of SecANT

Entry added February 5, 2025

WebKit

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: Processing web content may lead to arbitrary code execution

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 259694

CVE-2024-23226: Pwn2car

WebKit Bugzilla: 263001

CVE-2024-27859: Pwn2car

Entry added March 7, 2024, updated February 5, 2025

WebKit

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: A malicious website may exfiltrate audio data cross-origin

Description: The issue was addressed with improved UI handling.

WebKit Bugzilla: 263795

CVE-2024-23254: James Lee (@Windowsrcer)

Entry added March 7, 2024

WebKit

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

WebKit

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: A maliciously crafted webpage may be able to fingerprint the user

Description: An injection issue was addressed with improved validation.

WebKit Bugzilla: 266703

CVE-2024-23280: an anonymous researcher

Entry added March 7, 2024

WebKit

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

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

Additional recognition

AirDrop

We would like to acknowledge Cristian Dinca of "Tudor Vianu" National High School of Computer Science, Romania for their assistance.

CoreAnimation

We would like to acknowledge Junsung Lee for their assistance.

Entry added March 7, 2024

CoreMotion

We would like to acknowledge Eric Dorphy of Twin Cities App Dev LLC for their assistance.

Entry added March 7, 2024

Find My

We would like to acknowledge Meng Zhang (鲸落) of NorthSea for their assistance.

Entry added March 7, 2024

ICU

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

Entry added February 5, 2025

Kernel

We would like to acknowledge Tarek Joumaa (@tjkr0wn) and 이준성(Junsung Lee) for their assistance.

Entry added March 7, 2024

libxml2

We would like to acknowledge OSS-Fuzz, and Ned Williamson of Google Project Zero for their assistance.

Entry added March 7, 2024

libxpc

We would like to acknowledge Rasmus Sten, F-Secure (Mastodon: @pajp@blog.dll.nu), and an anonymous researcher for their assistance.

Entry added March 7, 2024

Mail Conversation View

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

Messages

We would like to acknowledge Petar Mataić for their assistance.

Entry added February 5, 2025

NetworkExtension

We would like to acknowledge Mathy Vanhoef (KU Leuven University) for their assistance.

Photos

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) of Lakshmi Narain College Of Technology Bhopal for their assistance.

Entry added March 7, 2024

Power Management

We would like to acknowledge Pan ZhenPeng (@Peterpan0927) of STAR Labs SG Pte. Ltd. for their assistance.

Entry added March 7, 2024

Safari

We would like to acknowledge Abhinav Saraswat and Matthew C for their assistance.

Entry added March 7, 2024

Sandbox

We would like to acknowledge Zhongquan Li (@Guluisacat) for their assistance.

Entry added March 7, 2024

Settings

We would like to acknowledge Christian Scalese, Logan Ramgoon, Lucas Monteiro, Daniel Monteiro, Felipe Monteiro, and Peter Watthey for their assistance.

Shortcuts

We would like to acknowledge Yusuf Kelany for their assistance.

Entry added July 29, 2024

Siri

We would like to acknowledge Bistrit Dahal for their assistance.

Entry added March 7, 2024

Software Update

We would like to acknowledge Bin Zhang of Dublin City University for their assistance.

Entry added March 7, 2024

WebKit

We would like to acknowledge Nan Wang (@eternalsakura13) of 360 Vulnerability Research Institute, Valentino Dalla Valle, Pedro Bernardo, Marco Squarcina, and Lorenzo Veronese of TU Wien for their assistance.

Entry added March 7, 2024

WebRTC

We would like to acknowledge Narendra Bhati From Suma Soft Pvt. Ltd, Pune (India) - twitter.com/imnarendrabhati for their assistance.

Entry added February 5, 2025

Published Date: February 05, 2025