About the security content of watchOS 10.4

This document describes the security content of watchOS 10.4.

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.

watchOS 10.4

Released March 7, 2024

Accessibility

Available for: Apple Watch Series 4 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

AppleMobileFileIntegrity

Available for: Apple Watch Series 4 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)

CoreBluetooth - LE

Available for: Apple Watch Series 4 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)

file

Available for: Apple Watch Series 4 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

ImageIO

Available for: Apple Watch Series 4 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 updated May 31, 2024

Kernel

Available for: Apple Watch Series 4 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

Kernel

Available for: Apple Watch Series 4 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

Kernel

Available for: Apple Watch Series 4 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

libxpc

Available for: Apple Watch Series 4 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

libxpc

Available for: Apple Watch Series 4 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

MediaRemote

Available for: Apple Watch Series 4 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

Messages

Available for: Apple Watch Series 4 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)

RTKit

Available for: Apple Watch Series 4 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

Sandbox

Available for: Apple Watch Series 4 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)

Sandbox

Available for: Apple Watch Series 4 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)

Share Sheet

Available for: Apple Watch Series 4 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)

Siri

Available for: Apple Watch Series 4 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

Siri

Available for: Apple Watch Series 4 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

UIKit

Available for: Apple Watch Series 4 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

WebKit

Available for: Apple Watch Series 4 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: Apple Watch Series 4 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: Apple Watch Series 4 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)

WebKit

Available for: Apple Watch Series 4 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)

WebKit

Available for: Apple Watch Series 4 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

WebKit

Available for: Apple Watch Series 4 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

Additional recognition

CoreAnimation

We would like to acknowledge Junsung Lee for their assistance.

CoreMotion

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

Find My

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

Kernel

We would like to acknowledge Tarek Joumaa (@tjkr0wn) for their assistance.

libxml2

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

libxpc

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

Messages

We would like to acknowledge Petar Mataić for their assistance.

Entry added February 5, 2025

Power Management

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

Sandbox

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

Siri

We would like to acknowledge Bistrit Dahal for their assistance.

Software Update

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

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.

Published Date: February 05, 2025

Helpful? Yes No