About the security content of watchOS 10.3

This document describes the security content of watchOS 10.3.

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 10.3

Released January 22, 2024

Apple Neural Engine

Available for devices with Apple Neural Engine: Apple Watch Series 9 and Apple Watch Ultra 2

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

Description: The issue was addressed with improved memory handling.

CVE-2024-23212: Ye Zhang of Baidu Security

CoreCrypto

Available for: Apple Watch Series 4 and later

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

Kernel

Available for: Apple Watch Series 4 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-2024-23208: fmyy(@binary_fmyy) and lime From TIANGONG Team of Legendsec at QI-ANXIN Group

libxpc

Available for: Apple Watch Series 4 and later

Impact: An app may be able to cause a denial-of-service

Description: A permissions issue was addressed with additional restrictions.

CVE-2024-23201: Koh M. Nakagawa of FFRI Security, Inc. and an anonymous researcher

Entry added March 7, 2024

Mail Search

Available for: Apple Watch Series 4 and later

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

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

CVE-2024-23207: Noah Roskin-Frazee and Prof. J. (ZeroClicks.ai Lab), and Ian de Marcellus

NSSpellChecker

Available for: Apple Watch Series 4 and later

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

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

CVE-2024-23223: Noah Roskin-Frazee and Prof. J. (ZeroClicks.ai Lab)

Safari

Available for: Apple Watch Series 4 and later

Impact: A user's private browsing activity may be visible in Settings

Description: A privacy issue was addressed with improved handling of user preferences.

CVE-2024-23211: Mark Bowers

Shortcuts

Available for: Apple Watch Series 4 and later

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)

Shortcuts

Available for: Apple Watch Series 4 and later

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

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

CVE-2024-23217: Kirin (@Pwnrin)

TCC

Available for: Apple Watch Series 4 and later

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

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

CVE-2024-23215: Zhongquan Li (@Guluisacat)

Time Zone

Available for: Apple Watch Series 4 and later

Impact: An app may be able to view a user's phone number in system logs

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

CVE-2024-23210: Noah Roskin-Frazee and Prof. J. (ZeroClicks.ai Lab)

WebKit

Available for: Apple Watch Series 4 and later

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

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

WebKit Bugzilla: 262699

CVE-2024-23206: an anonymous researcher

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: 266619

CVE-2024-23213: Wangtaiyu of Zhongfu info

WebKit

Available for: Apple Watch Series 4 and later

Impact: A malicious website may cause unexpected cross-origin behavior

Description: A logic issue was addressed with improved checks.

WebKit Bugzilla: 265812

CVE-2024-23271: James Lee (@Windowsrcer)

Entry added April 24, 2024

Additional recognition

NetworkExtension

We would like to acknowledge Nils Rollshausen for their assistance.

Entry added April 24, 2024

Published Date: July 03, 2024