

About the security content of iOS 16.7.5 and iPadOS 16.7.5

This document describes the security content of iOS 16.7.5 and iPadOS 16.7.5.

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 16.7.5 and iPadOS 16.7.5

Released January 22, 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 access sensitive user data

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

CVE-2023-42937: Noah Roskin-Frazeo and Prof. J. (ZeroClicks.ai Lab)

Apple Neural Engine

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 execute arbitrary code with kernel privileges

Description: The issue was addressed with improved memory handling.

CVE-2024-23212: Ye Zhang of Baidu Security

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 a maliciously crafted image may result in disclosure of process memory

Description: The issue was addressed with improved checks.

CVE-2023-42888: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Power Manager

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 corrupt coprocessor memory

Description: The issue was addressed with improved checks.

CVE-2024-27791: Pan ZhenPeng (@Peterpan0927) of STAR Labs SG Pte. Ltd.

Entry added April 24, 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: 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

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 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: 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 lead to arbitrary code execution

Description: Multiple memory corruption issues were addressed with improved memory handling.

WebKit Bugzilla: 265129

CVE-2024-23214: Nan Wang (@eternalsakura13) of 360 Vulnerability Research Institute

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: 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: 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 lead to arbitrary code execution. Apple is aware of a report that this issue may have been exploited.

Description: A type confusion issue was addressed with improved checks.

WebKit Bugzilla: 267134

CVE-2024-23222

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. [Contact the vendor](#) for additional information.

Published Date: June 03, 2024

Helpful?

Yes

No

Apple > Support > About the security content of iOS 16.7.5 and iPadOS 16.7.5