About the security content of iOS 18.2 and iPadOS 18.2

This document describes the security content of iOS 18.2 and iPadOS 18.2.

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 18.2 and iPadOS 18.2

Released December 11, 2024

AppleMobileFileIntegrity

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: The issue was addressed with improved checks.

CVE-2024-54526: Mickey Jin (@patch1t), Arsenii Kostromin (0x3c3e)

AppleMobileFileIntegrity

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: This issue was addressed with improved checks.

CVE-2024-54527: Mickey Jin (@patch1t)

Audio

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: Muting a call while ringing may not result in mute being enabled

Description: An inconsistent user interface issue was addressed with improved state management.

CVE-2024-54503: Micheal Chukwu and an anonymous researcher

Crash Reporter

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: A permissions issue was addressed with additional restrictions.

CVE-2024-54513: an anonymous researcher

FontParser

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: Processing a maliciously crafted font may result in the disclosure of process memory

Description: The issue was addressed with improved checks.

CVE-2024-54486: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

ImageIO

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: Processing a maliciously crafted image may result in disclosure of process memory

Description: The issue was addressed with improved checks.

CVE-2024-54500: Junsung Lee working with Trend Micro Zero Day Initiative

Kernel

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: An attacker may be able to create a read-only memory mapping that can be written to

Description: A race condition was addressed with additional validation.

CVE-2024-54494: sohybbyk

Kernel

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to leak sensitive kernel state

Description: A race condition was addressed with improved locking.

CVE-2024-54510: Joseph Ravichandran (@0xjprx) of MIT CSAIL

Kernel

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

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

Description: The issue was addressed with improved memory handling.

CVE-2024-44245: an anonymous researcher

libexpat

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: A remote attacker may cause an unexpected app termination or arbitrary code execution

Description: This is a vulnerability in open source code and Apple Software is among the affected projects. The CVE-ID was assigned by a third party. Learn more about the issue and CVE-ID at cve.org.

CVE-2024-45490

libxpc

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th 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-2024-54514: an anonymous researcher

libxpc

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to gain elevated privileges

Description: A logic issue was addressed with improved checks.

CVE-2024-44225: 风沐云烟(@binary_fmyy)

Passwords

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: An attacker in a privileged network position may be able to alter network traffic

Description: This issue was addressed by using HTTPS when sending information over the network.

CVE-2024-54492: Talal Haj Bakry and Tommy Mysk of Mysk Inc. (@mysk_co)

Safari

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: On a device with Private Relay enabled, adding a website to the Safari Reading List may reveal the originating IP address to the website

Description: The issue was addressed with improved routing of Safari-originated requests.

CVE-2024-44246: Jacob Braun

SceneKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: Processing a maliciously crafted file may lead to a denial of service

Description: The issue was addressed with improved checks.

CVE-2024-54501: Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative

VoiceOver

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: An attacker with physical access to an iOS device may be able to view notification content from the lock screen

Description: The issue was addressed by adding additional logic.

CVE-2024-54485: Abhay Kailasia (@abhay_kailasia) from C-DAC Thiruvananthapuram India

WebKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: Processing maliciously crafted web content may lead to an unexpected process crash

Description: The issue was addressed with improved checks.

WebKit Bugzilla: 278497

CVE-2024-54479: Seunghyun Lee

WebKit Bugzilla: 281912

CVE-2024-54502: Brendon Tiszka of Google Project Zero

WebKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: Processing maliciously crafted web content may lead to an unexpected process crash

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 282180

CVE-2024-54508: linjy of HKUS3Lab and chluo of WHUSecLab, Xiangwei Zhang of Tencent Security YUNDING LAB

WebKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: Processing maliciously crafted web content may lead to memory corruption

Description: A type confusion issue was addressed with improved memory handling.

WebKit Bugzilla: 282661

CVE-2024-54505: Gary Kwong

WebKit

Available for: iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later

Impact: Processing maliciously crafted web content may lead to memory corruption

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 277967

CVE-2024-54534: Tashita Software Security

Additional recognition

Accessibility

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) of Lakshmi Narain College of Technology Bhopal India, Andr.Ess, Jake Derouin, Jason Gendron (@gendron_jason) for their assistance.

App Protection

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

Calendar

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

FaceTime

We would like to acknowledge 椰椰 for their assistance.

FaceTime Foundation

We would like to acknowledge Joshua Pellecchia for their assistance.

Family Sharing

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

Notes

We would like to acknowledge Katzenfutter for their assistance.

Photos

We would like to acknowledge Bistrit Dahal, Chi Yuan Chang of ZUSO ART and taikosoup, Finlay James (@Finlay1010), Rizki Maulana (rmrizki.my.id), Srijan Poudel for their assistance.

Photos Storage

We would like to acknowledge Jake Derouin (jakederouin.com) for their assistance.

Proximity

We would like to acknowledge Junming C. (@Chapoly1305) and Prof. Qiang Zeng of George Mason University for their assistance.

Quick Response

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

Safari

We would like to acknowledge Jayateertha Guruprasad for their assistance.

Safari Private Browsing

We would like to acknowledge Richard Hyunho Im (@richeeta) with Route Zero Security for their assistance.

Settings

We would like to acknowledge Akshith Muddasani, Bistrit Dahal, Emanuele Slusarz for their assistance.

Siri

We would like to acknowledge Srijan Poudel for their assistance.

Spotlight

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) from LNCT Bhopal and C-DAC Thiruvananthapuram India for their assistance.

Status Bar

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

Swift

We would like to acknowledge Marc Schoenefeld, Dr. rer. nat. for their assistance.

Time Zone

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) from LNCT Bhopal and C-DAC Thiruvananthapuram India for their assistance.

WebKit

We would like to acknowledge Hafiizh for their assistance.

WindowServer

We would like to acknowledge Felix Kratz for their assistance.

Published Date: December 11, 2024