About the security content of iOS 15 and iPadOS 15

This document describes the security content of iOS 15 and iPadOS 15.

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 updates page.

Apple security documents reference vulnerabilities by CVE-ID when possible.

For more information about security, see the Apple Product Security page.

iOS 15 and iPadOS 15

Released September 20, 2021

Accessory Manager

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

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

Description: A memory consumption issue was addressed with improved memory handling.

CVE-2021-30837: Siddharth Aeri (@b1n4r1b01)

AppleMobileFileIntegrity

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: A local attacker may be able to read sensitive information

Description: This issue was addressed with improved checks.

CVE-2021-30811: an anonymous researcher working with Compartir

Apple Neural Engine

Available for devices with Apple Neural Engine: iPhone 8 and later, iPad Pro (3rd generation) and later, iPad Air (3rd generation) and later, and iPad mini (5th generation)

Impact: A malicious application may be able to execute arbitrary code with system privileges on devices with an Apple Neural Engine

Description: A memory corruption issue was addressed with improved memory handling.

CVE-2021-30838: proteas wang

CoreML

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: A local attacker may be able to cause unexpected application termination or arbitrary code execution

Description: This issue was addressed with improved checks.

CVE-2021-30825: hjy79425575 working with Trend Micro Zero Day Initiative

Face ID

Available for devices with Face ID: iPhone X, iPhone XR, iPhone XS (all models), iPhone 11 (all models), iPhone 12 (all models), iPad Pro (11-inch), and iPad Pro (3rd generation)

Impact: A 3D model constructed to look like the enrolled user may be able to authenticate via Face ID

Description: This issue was addressed by improving Face ID anti-spoofing models.

CVE-2021-30863: Wish Wu (吴潍浠 @wish_wu) of Ant-financial Light-Year Security Lab

FontParser

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing a maliciously crafted dfont file may lead to arbitrary code execution

Description: This issue was addressed with improved checks.

CVE-2021-30841: Xingwei Lin of Ant Security Light-Year Lab

CVE-2021-30842: Xingwei Lin of Ant Security Light-Year Lab

CVE-2021-30843: Xingwei Lin of Ant Security Light-Year Lab

ImageIO

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing a maliciously crafted image may lead to arbitrary code execution

Description: This issue was addressed with improved checks.

CVE-2021-30835: Ye Zhang of Baidu Security

CVE-2021-30847: Mike Zhang of Pangu Lab

Kernel

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: A malicious application may be able to execute arbitrary code with kernel privileges

Description: A race condition was addressed with improved locking.

CVE-2021-30857: Zweig of Kunlun Lab

libexpat

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: A remote attacker may be able to cause a denial of service

Description: This issue was addressed by updating expat to version 2.4.1.

CVE-2013-0340: an anonymous researcher

Model I/O

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing a maliciously crafted USD file may disclose memory contents

Description: An out-of-bounds read was addressed with improved input validation.

CVE-2021-30819: Apple

Preferences

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: An application may be able to access restricted files

Description: A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks.

CVE-2021-30855: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020) of Tencent Security Xuanwu Lab (xlab.tencent.com)

Preferences

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: A sandboxed process may be able to circumvent sandbox restrictions

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

CVE-2021-30854: Zhipeng Huo (@R3dF09) and Yuebin Sun (@yuebinsun2020) of Tencent Security Xuanwu Lab (xlab.tencent.com)

Siri

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: A local attacker may be able to view contacts from the lock screen

Description: A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management.

CVE-2021-30815: an anonymous researcher

Telephony

Available for: iPhone SE (1st generation), iPad Pro 12.9-inch, iPad Air 2, iPad (5th generation), and iPad mini 4

Impact: In certain situations, the baseband would fail to enable integrity and ciphering protection

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

CVE-2021-30826: CheolJun Park, Sangwook Bae and BeomSeok Oh of KAIST SysSec Lab

WebKit

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to arbitrary code execution

Description: A memory corruption issue was addressed with improved memory handling.

CVE-2021-30846: Sergei Glazunov of Google Project Zero

WebKit

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to code execution

Description: A memory corruption issue was addressed with improved memory handling.

CVE-2021-30848: Sergei Glazunov of Google Project Zero

WebKit

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to arbitrary code execution

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

CVE-2021-30849: Sergei Glazunov of Google Project Zero

WebKit

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to code execution

Description: A memory corruption vulnerability was addressed with improved locking.

CVE-2021-30851: Samuel Groß of Google Project Zero

Wi-Fi

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: An attacker in physical proximity may be able to force a user onto a malicious Wi-Fi network during device setup

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

CVE-2021-30810: an anonymous researcher

Additional recognition

Assets

We would like to acknowledge Cees Elzinga for their assistance.

Bluetooth

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

File System

We would like to acknowledge Siddharth Aeri (@b1n4r1b01) for their assistance.

Sandbox

We would like to acknowledge Csaba Fitzl (@theevilbit) of Offensive Security for their assistance.

UIKit

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

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.

Julkaisupäivämäärä: 20. syyskuuta 2021

Oliko tästä hyötyä? Kyllä Ei