About the security content of iOS 26.2 and iPadOS 26.2

This document describes the security content of iOS 26.2 and iPadOS 26.2.

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 26.2 and iPadOS 26.2

Released December 12, 2025

App Store

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to access sensitive payment tokens

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-46288: floeki, Zhongcheng Li from IES Red Team of ByteDance

AppleJPEG

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: Processing a file may lead to memory corruption

Description: The issue was addressed with improved bounds checks.

CVE-2025-43539: Michael Reeves (@IntegralPilot)

BiometricKit

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later

Impact: Restoring from a backup may prevent passcode from being required immediately after Face ID enrollment

Description: A logic issue was addressed with improved validation.

CVE-2025-46286: Andrei Simion

Entry added January 9, 2026

Books

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: Restoring a maliciously crafted backup file may lead to modification of protected system files

Description: A path handling issue was addressed with improved validation.

CVE-2025-43537: piffz, Daniel Nurkin, Al Sadman Awal, Mohamed Hamdadou & Mahran Alhazmi, Hichem Maloufi, Christian Mina, Gerson Aldaz, qwerty j0y & Ricardo Garcia, Dorian Del Valle

Entry added February 11, 2026, updated March 24, 2026

Calling Framework

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: An attacker may be able to spoof their FaceTime caller ID

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

CVE-2025-46287: an anonymous researcher, Riley Walz

curl

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: Multiple issues in curl

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-2024-7264

CVE-2025-9086

FaceTime

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: Password fields may be unintentionally revealed when remotely controlling a device over FaceTime

Description: This issue was addressed with improved state management.

CVE-2025-43542: Yiğit Ocak

Foundation

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to inappropriately access files through the spellcheck API

Description: A logic issue was addressed with improved checks.

CVE-2025-43518: Noah Gregory (wts.dev)

Foundation

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: Processing malicious data may lead to unexpected app termination

Description: A memory corruption issue was addressed with improved bounds checking.

CVE-2025-43532: Andrew Calvano and Lucas Pinheiro of Meta Product Security

Icons

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to identify what other apps a user has installed

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-46279: Duy Trần (@khanhduytran0)

iTunes Store

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: A user with physical access to an iOS device may be able to bypass Activation Lock

Description: A path handling issue was addressed with improved validation.

CVE-2025-43534: iG0x72 and JJ of XiguaSec, Lehan Dilusha Jayasinghe

Entry added March 24, 2026

Kernel

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to gain root privileges

Description: An integer overflow was addressed by adopting 64-bit timestamps.

CVE-2025-46285: Kaitao Xie and Xiaolong Bai of Alibaba Group

libarchive

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: Processing a file may lead to memory corruption

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-2025-5918

MediaExperience

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

Description: A logging issue was addressed with improved data redaction.

CVE-2025-43475: Rosyna Keller of Totally Not Malicious Software

Messages

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

Description: An information disclosure issue was addressed with improved privacy controls.

CVE-2025-46276: Rosyna Keller of Totally Not Malicious Software

Multi-Touch

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: A malicious HID device may cause an unexpected process crash

Description: The issue was addressed with improved bounds checks.

CVE-2025-43533: Google Threat Analysis Group

CVE-2025-46300: Google Threat Analysis Group

CVE-2025-46301: Google Threat Analysis Group

CVE-2025-46302: Google Threat Analysis Group

CVE-2025-46303: Google Threat Analysis Group

CVE-2025-46304: Google Threat Analysis Group

CVE-2025-46305: Google Threat Analysis Group

Entry updated February 11, 2026

Photos

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: Photos in the Hidden Photos Album may be viewed without authentication

Description: A configuration issue was addressed with additional restrictions.

CVE-2025-43428: an anonymous researcher, Michael Schmutzer of Technische Hochschule Ingolstadt

Screen Time

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to access a user's Safari history

Description: A logging issue was addressed with improved data redaction.

CVE-2025-46277: Kirin (@Pwnrin)

Screen Time

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

Description: A logging issue was addressed with improved data redaction.

CVE-2025-43538: Iván Savransky

Security

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

Description: A logic issue was addressed with improved checks.

CVE-2025-46290: Bing Shi, Wenchao Li and Xiaolong Bai of Alibaba Group, and Luyi Xing of Indiana University Bloomington

Entry added February 11, 2026

Telephony

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

Description: This issue was addressed with additional entitlement checks.

CVE-2025-46292: Rosyna Keller of Totally Not Malicious Software

WebKit

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

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

WebKit Bugzilla: 301257

CVE-2025-43541: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

WebKit

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

Description: A use-after-free issue was addressed with improved memory management.

WebKit Bugzilla: 301726

CVE-2025-43536: Nan Wang (@eternalsakura13)

WebKit

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th 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: 300774

CVE-2025-43535: Google Big Sleep, Nan Wang (@eternalsakura13)

WebKit Bugzilla: 301468

CVE-2025-46298: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative, Nan Wang (@eternalsakura13)

Entry updated January 9, 2026

WebKit

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

Description: A buffer overflow issue was addressed with improved memory handling.

WebKit Bugzilla: 301371

CVE-2025-43501: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

WebKit

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

Description: A race condition was addressed with improved state handling.

WebKit Bugzilla: 301940

CVE-2025-43531: Phil Pizlo of Epic Games

WebKit

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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 in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 26. CVE-2025-14174 was also issued in response to this report.

Description: A use-after-free issue was addressed with improved memory management.

WebKit Bugzilla: 302502

CVE-2025-43529: Google Threat Analysis Group

WebKit

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: Processing maliciously crafted web content may lead to memory corruption. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 26. CVE-2025-43529 was also issued in response to this report.

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

WebKit Bugzilla: 303614

CVE-2025-14174: Apple and Google Threat Analysis Group

WebKit

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and

later, and iPad mini 5th generation and later

Impact: Processing maliciously crafted web content may disclose internal states of the app

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

WebKit Bugzilla: 299518

CVE-2025-46299: Google Big Sleep

Entry added January 9, 2026

WebKit Web Inspector

Available for: iPhone 11 and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

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

Description: A use-after-free issue was addressed with improved memory management.

WebKit Bugzilla: 300926

CVE-2025-43511: 이동하 (Lee Dong Ha of BoB 14th)

Additional recognition

AppleMobileFileIntegrity

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

Core Services

We would like to acknowledge Golden Helm Securities, Csaba Fitzl (@theevilbit) of Iru and Gergely Kalman (@gergely_kalman) for their assistance.

Entry updated January 9, 2026

Safari

We would like to acknowledge Mochammad Nosa Shandy Prastyo for their assistance.

Siri

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

WebKit

We would like to acknowledge Geva Nurgandi Syahputra (gevakun) and Google Big Sleep for their assistance.

Entry updated January 9, 2026

Published Date: March 24, 2026

Helpful? Yes No

