About the security content of iOS 18.6 and iPadOS 18.6

This document describes the security content of iOS 18.6 and iPadOS 18.6.

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 18.6 and iPadOS 18.6

Released July 29, 2025

Accessibility

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: Passcode may be read aloud by VoiceOver

Description: A logic issue was addressed with improved checks.

CVE-2025-31229: Wong Wee Xiang

Accessibility

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: Privacy Indicators for microphone or camera access may not be correctly displayed

Description: The issue was addressed by adding additional logic.

CVE-2025-43217: Himanshu Bharti (@Xpl0itme)

afclip

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: Parsing a file may lead to an unexpected app termination

Description: The issue was addressed with improved memory handling.

CVE-2025-43186: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CFNetwork

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 non-privileged user may be able to modify restricted network settings

Description: A denial-of-service issue was addressed with improved input validation.

CVE-2025-43223: Andreas Jaegersberger & Ro Achterberg of Nosebeard Labs

CoreAudio

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 audio file may lead to memory corruption

Description: The issue was addressed with improved memory handling.

CVE-2025-43277: Google's Threat Analysis Group

CoreMedia

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 media file may lead to unexpected app termination or corrupt process memory

Description: An out-of-bounds access issue was addressed with improved bounds checking.

CVE-2025-43210: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreMedia Playback

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 user-sensitive data

Description: The issue was addressed with additional permissions checks.

CVE-2025-43230: Chi Yuan Chang of ZUSO ART and taikosoup

ICU

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 Safari crash

Description: An out-of-bounds access issue was addressed with improved bounds checking.

CVE-2025-43209: Gary Kwong working with 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: An out-of-bounds read was addressed with improved input validation.

CVE-2025-43226

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

Description: A double free issue was addressed with improved memory management.

CVE-2025-43282: Christian Kohlschütter

Entry added October 15, 2025

libnetcore

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 file may lead to memory corruption

Description: This issue was addressed with improved memory handling.

CVE-2025-43202: Brian Carpenter

libxml2

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 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-2025-7425: Sergei Glazunov of Google Project Zero

libxslt

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: 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-2025-7424: Ivan Fratric of Google Project Zero

Mail Drafts

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: Remote content may be loaded even when the 'Load Remote Images' setting is turned off

Description: This issue was addressed through improved state management.

CVE-2025-31276: Himanshu Bharti (@Xpl0itme)

Mail Drafts

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: Forwarding an email could display remote images in Mail in Lockdown Mode

Description: The issue was resolved by not loading remote images

CVE-2025-43280: Himanshu Bharti @Xpl0itme

Entry added October 15, 2025

Metal

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 texture may lead to unexpected app termination

Description: Multiple memory corruption issues were addressed with improved input validation.

CVE-2025-43234: Vlad Stolyarov of Google's Threat Analysis Group

Model I/O

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 media file may lead to unexpected app termination or corrupt process memory

Description: An out-of-bounds access issue was addressed with improved bounds checking.

CVE-2025-43224: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

CVE-2025-43221: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

Model I/O

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 unexpected app termination

Description: An input validation issue was addressed with improved memory handling.

CVE-2025-31281: Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative

SQLite

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 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-2025-6965

Entry added October 15, 2025

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: Visiting a malicious website may lead to address bar spoofing

Description: The issue was addressed with improved UI.

WebKit Bugzilla: 294374

CVE-2025-43228: Jaydev Ahire

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 disclose sensitive user information

Description: This issue was addressed through improved state management.

WebKit Bugzilla: 292888

CVE-2025-43227: Gilad Moav, Yehuda Afek, Anat Bremler-Barr, and Amit Klein

Entry updated October 15, 2025

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: 291742

CVE-2025-31278: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

WebKit Bugzilla: 291745

CVE-2025-31277: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

WebKit Bugzilla: 293579

CVE-2025-31273: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

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 Safari crash

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 292599

CVE-2025-43214: shandikri working with Trend Micro Zero Day Initiative, Google V8 Security Team

WebKit Bugzilla: 292621

CVE-2025-43213: Google V8 Security Team

WebKit Bugzilla: 293197

CVE-2025-43212: Nan Wang (@eternalsakura13) and Ziling Chen

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 web content may lead to a denial-of-service

Description: The issue was addressed with improved memory handling.

WebKit Bugzilla: 293730

CVE-2025-43211: Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei

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 disclose internal states of the app

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

WebKit Bugzilla: 294182

CVE-2025-43265: HexRabbit (@h3xr4bb1t) from DEVCORE Research Team

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 Safari crash

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

WebKit Bugzilla: 295382

CVE-2025-43216: Ignacio Sanmillan (@ulexec)

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 Safari crash

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.

WebKit Bugzilla: 296459

CVE-2025-6558: Clément Lecigne and Vlad Stolyarov of Google's Threat Analysis Group

Additional recognition

Accessibility

We would like to acknowledge Abhay Kailasia (@abhay_kailasia) from C-DAC Thiruvananthapuram India, Hamza BHP, Himanshu Bharti (@Xpl0itme) for their assistance.

Activation Lock

We would like to acknowledge salemdomain for their assistance.

Bluetooth

We would like to acknowledge LIdong LI, Xiao Wang, Shao Dong Chen, and Chao Tan of Source Guard for their assistance.

CoreAudio

We would like to acknowledge Noah Weinberg for their assistance.

Device Management

We would like to acknowledge Al Karak for their assistance.

libxml2

We would like to acknowledge Sergei Glazunov of Google Project Zero for their assistance.

libxslt

We would like to acknowledge Ivan Fratric of Google Project Zero for their assistance.

Managed Configuration

We would like to acknowledge Bill Marczak of The Citizen Lab at The University of Toronto's Munk School for their assistance.

MobileGestalt

We would like to acknowledge Hana Kim (@hanakim3945) of XiguaSec for their assistance.

Entry added October 15, 2025

Photos

We would like to acknowledge Chaojie Peng (彭超杰), Dalibor Milanovic for their assistance.

Entry updated October 15, 2025

Safari

We would like to acknowledge Ameen Basha M K for their assistance.

Shortcuts

We would like to acknowledge Dennis Kniep for their assistance.

Siri

We would like to acknowledge Timo Hetzel for their assistance.

WebKit

We would like to acknowledge Google V8 Security Team, Yuhao Hu, Yan Kang, Chenggang Wu, and Xiaojie Wei, rheza (@ginggilBesel) for their assistance.

Published Date: October 15, 2025