iOS 18.6 has important security fixes, here are the full details

Ryan Christoffel | Jul 29 2025 - 10:58 am PT

Apple has just released iOS 18.6, the latest iPhone update for users. Though anyone hoping for big new features will have to wait for iOS 26 this fall, today's new iOS 18.6 release does provide a host of important security fixes. Here are the full details.

Installing iOS 18.6 on your iPhone

We all have our own reasons for installing iOS updates. For some, it's compelling new features we want to try. For others, the need to stop our iPhone from bugging us with pop-up alerts.

Whatever your reason, iOS 18.6 is recommended for all users because of the "important bug fixes and security updates" it provides.

You can access and install the update by opening Settings → General → Software Update on your iPhone.

Though you may not feel like your data or security is at risk, Apple has packed iOS 18.6 full of fixes that help ensure things stay that way.

Here are the full release notes for iOS and iPadOS 18.6's security fixes. You can find details for today's other updates here.

iOS 18.6: Apple's full security release notes

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

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)

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

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

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