

About the security content of visionOS 2.6

This document describes the security content of visionOS 2.6.

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.

visionOS 2.6

Released July 29, 2025

afclip

Available for: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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

libxml2

Available for: Apple Vision Pro

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: Apple Vision Pro

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

Metal

Available for: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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: Apple Vision Pro

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

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.

Shortcuts

We would like to acknowledge Dennis Kniep 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.


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.

Published Date: October 15, 2025

Helpful?

Yes

No

 > Support > About the security content of visionOS 2.6

Copyright © 2026 Apple Inc. All rights reserved. [Privacy Policy](#) | [Terms of Use](#) | [Sales and Refunds](#) | [Site Map](#)

United States