March 7, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Apple published security updates to address vulnerabilities in the following products:

- macOS Monterey – versions prior to 12.7.4
- macOS Sonoma – versions prior to 14.4
- macOS Ventura – versions prior to 13.6.5
- Safari – versions prior to 17.4
- tvOS – versions prior to 17.4
- visionOS – versions prior to 1.1
- watchOS – versions prior to 10.4

Apple has received reports that CVE-2024-23225 and CVE-2024-23296 have been exploited.

Technical Details
Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Kernel

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited.

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

CVE-2024-23225

RTKit

Available for: iPhone XS and later, iPad Pro 12.9-inch 2nd generation and later, iPad Pro 10.5-inch, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 6th generation and later, and iPad mini 5th generation and later

Impact: An attacker with arbitrary kernel read and write capability may be able to bypass kernel memory protections. Apple is aware of a report that this issue may have been exploited.

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

CVE-2024-23296

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-23273 CVE-2024-23252 CVE-2024-23254 CVE-2024-23263 CVE-2024-23280 CVE-2024-23284 CVE-2024-23291 CVE-2024-23257 CVE-2024-23258 CVE-2024-23286 CVE-2024-23235 CVE-2024-23265 CVE-2024-23225 CVE-2024-23264 CVE-2024-23295 CVE-2024-23296 CVE-2024-23220 CVE-2024-23246 CVE-2024-23226 CVE-2024-23263 CVE-2024-23288 CVE-2024-23250 CVE-2022-48554 CVE-2024-23286 CVE-2024-23235 CVE-2024-23225 CVE-2024-23278 CVE-2024-0258 CVE-2024-23297 CVE-2024-23287 CVE-2024-23239 CVE-2024-23290 CVE-2024-23231 CVE-2024-23289 CVE-2024-23293 CVE-2024-23280
- Apple Security Updates