March 6, 2024

Overall rating: Critical

BRITISH COLUMBIA

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:

- iOS and iPadOS – versions prior to 17.4
- iOS and iPadOS – versions prior to 16.7.6

Apple has received reports that CVE-2024-23225 and CVE-2024-23296 have been exploited. Exploitation of these vulnerabilities could lead to a bypass of kernel memory protections.

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-2024-23243 CVE-2024-23225 CVE-2024-23296 CVE-2024-23256
- About the security content of iOS 17.4 and iPadOS 17.4
- About the security content of iOS 16.7.6 and iPadOS 16.7.6
- Apple Security Updates