January 22, 2024

Overall Rating - High

This notification is intended as an informational bulletin 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 17.3
- iOS and iPadOS – versions prior to 16.7.5
- iOS and iPadOS – versions prior to 15.8.1
- macOS Sonoma – versions prior to 14.3
- macOS Ventura – versions prior to 13.6.4
- macOS Monterey – versions prior to 12.7.3
- watchOS – versions prior to 10.3
- tvOS – versions prior to 17.3

Exploitation of this vulnerability could result in a denial of service or execution of arbitrary code.

Technical Details

Available for devices with Apple Neural Engine: iPhone XS and later, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 8th generation and later, and iPad mini 5th generation and later

Impact: An app may be able to execute arbitrary code with kernel privileges
Description: The issue was addressed with improved memory handling.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

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

References

- CVE-2024-23212, CVE-2024-23218, CVE-2024-23208, CVE-2024-23207,CVE-2024-23223, CVE-2024-23219, CVE-2024-23211, CVE-2024-23203, CVE-2024-23204, CVE-2024-23217, CVE-2024-23215, CVE-2024-23210, CVE-2024-23213, CVE-2024-23214, CVE-2024-23222
- Apple Security Updates