May 14, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Apple published a security update to address a vulnerability in the following product:

- Safari – versions prior to 17.5

Technical Details

Apple has released security updates to fix a zero-day vulnerability in the Safari web browser exploited during this year's Pwn2Own Vancouver hacking competition.

The company addressed the security flaw (tracked as CVE-2024-27834) on systems running macOS Monterey and macOS Ventura with improved checks.

"An attacker with arbitrary read and write capability may be able to bypass Pointer Authentication," Apple explains in a Monday advisory.

Pointer authentication codes (PACs) are used on the arm64e architecture to detect and guard against unexpected changes to pointers in memory, with the CPU triggering app crashes following memory corruption events linked to authentication failures.

While Safari 17.5 is also available for iOS 17.5, iPadOS 17.5, macOS Sonoma 14.5, and visionOS 1.2, Apple has yet to confirm if it also patched the CVE-2024-27834 bug on these platforms.

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-2024-27834
- About the security content of Safari 17.5
- Apple Security Updates
- Apple fixes Safari WebKit zero-day flaw exploited at Pwn2Own (bleepingcomputer.com)