Security Advisory 2023-061

Zero-Click Vulnerabilities in Apple Operating Systems

September 8, 2023 — v1.0

TLP:CLEAR

History:

- *08/09/2023 — v1.0 – Initial publication*

Summary

In an article published on September 7 2023, *Citizen Lab* uncovered an actively exploited zero-click vulnerability used to deliver NSO Group's **Pegasus** spyware on an employee of a Washington DC based civil society organisation [1]. This exploit, named `BLASTPASS` could compromise iPhones running the latest iOS version without user interaction. The exploit involved `PassKit` attachments containing malicious images sent from an attacker iMessage account to the victim.

Citizen Lab promptly reported their findings to Apple, who issued two CVEs related to this exploit chain (CVE-2023-41064 and CVE-2023-41061). These vulnerabilities have now been patched in iOS, iPadOS, watchOS and macOS.

Technical Details

CVE-2023-41064

A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.5.2, iOS 16.6.1 and iPadOS 16.6.1. Processing a maliciously crafted image may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited [2].

CVE-2023-41061

A validation issue was addressed with improved logic. This issue is fixed in watchOS 9.6.2, iOS 16.6.1 and iPadOS 16.6.1. A maliciously crafted attachment may result in arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited [3].

Affected Products

MacOS Ventura, watchOS, iOS and iPadOS devices.

Recommendations

CERT-EU strongly recommends to update Apple devices.

Users who may face increased risk because of who they are or what they do could enable `Lockdown Mode` [4].

References

[1] https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/

[2] https://nvd.nist.gov/vuln/detail/CVE-2023-41064

[3] https://nvd.nist.gov/vuln/detail/CVE-2023-41061

[4] https://support.apple.com/en-ca/HT212650