Critical Apple Security Updates [1]

September 14, 2021

Summary

On September 13, 2021 Apple released security updates for supported versions of macOS Big Sur, macOS Catalina, macOS Mojave, iOS, iPadOS, watchOS, and Safari. The updates include a fix for an actively exploited no-click vulnerability. Exploitation of this vulnerability allows a remote attacker to take full control of the Apple device. Users of Apple devices should update their devices immediately.

Details

Security researchers at The Citizen Lab [2] disclosed the vulnerability (dubbed FORCEDENTRY) and the exploit code to Apple on Tuesday, September 7, 2021. The Citizen Lab determined a software developer supplying national governments used the vulnerability to remotely exploit and infect the latest Apple devices with the Pegasus spyware. “This spyware can do everything an iPhone user can do on their device and more,” said John Scott-Railton, a senior researcher at Citizen Lab, to The New York Times.

Apple lists the vulnerability as CVE-2021-30860, and described it as a maliciously crafted PDF that could lead to arbitrary code execution.

Devices specifically affected are those with iOS and iPadOS versions prior to 14.8, all devices running macOS versions prior to OSX Big Sur 11.6, and all Apple Watch devices running watchOS 7.6.2 or earlier.

References


Source URL: https://security.duke.edu/sep-2021-apple-patches

Links
[1] https://security.duke.edu/sep-2021-apple-patches