Hive Pro

THREAT ADVISORY

Apple fixes the zero-day vulnerabilities exploited by Pegasus spyware named "FORCEDENTRY“.

TA202132

Threat Level Red

Publish Date – September 16, 2021

Two actively exploited vulnerabilities (CVE-2021-30858 and CVE-2021-30860) have been fixed in Apple's iOS 14.8, iPadOS 14.8, watchOS 7.6.2, macOS Big Sur 11.6, and Safari 14.1.2 releases. The NSO group carried out the attack by simply sending a malicious text message which were actually Adobe PSD files that crashed the iMessage component responsible for automatically rendering images and then deployed the Pegasus surveillance tool. Users of Apple's iPhone, iPad, Mac, and Apple Watch should update their software right away to avoid any potential hazards resulting from active exploitation of the holes.

Vulnerability Details

CVE ID	Affected CPEs	Vulnerability Name
CVE-2021-30858	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*	Arbitrary code execution
CVE-2021-30860	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:* cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2020:*:*:*:*:*:* cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-004:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	Integer overflow leading to arbitrary code execution.

Threat Actor

Name	Known as	Origin	Target Locations	Target
NSO group	Pegasus spyware	Israel	Worldwide	Surveillance, Financial gain

Patch Links

https://support.apple.com/en-us/HT212804
https://support.apple.com/en-us/HT212805
https://support.apple.com/en-us/HT212806
https://support.apple.com/en-us/HT212807

References

https://thehackernews.com/2021/09/apple-issues-urgent-updates-to-fix-new.html
https://arstechnica.com/information-technology/2021/09/apple-fixes-imessage-zero-day-exploited-by-pegasus-spyware/