UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00218

NUMEROUS APPLE IOS VULNERABILITIES

DATE ISSUED: 1st November 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Multiple issues are under threat in unpatched Apple iOS devices that have the potential to lead to Remote Code Execution (RCE) attacks and privilege escalation to kernel level giving an attacker access to the Operating System.

BREAKDOWN

Apple has released a series of patches for devices prior to iOS14.8.1, iPadOS 14.8.1, watchOS 7.6.2 and tvOS 15.1, Safari 14.1.2 and macOS Big Sur 11.6 resolving a total of 24 CVEs, some of which are under known, active exploitation in the wild. Attackers are also able to exploit the vulnerabilities through the browser, making them susceptible to watering-hole attacks – a technique whereby attackers lure users to website to drop malware onto their devices. The vulnerabilities are across a number of areas including buffer overflow, memory corruption, out-of-bounds, logic and permission issues.

REMEDIATION STEPS

- Update to the latest version of iOS 15 available for your device

REFERENCES & RESOURCES

Threatpost https://threatpost.com/apple-patches-ios-bugs/175803/
CIS Advisory https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-remote-code-execution/
Apple https://support.apple.com/en-us/HT212868
https://support.apple.com/en-us/HT212869
https://support.apple.com/en-us/HT212872
https://support.apple.com/en-us/HT212871
https://support.apple.com/en-us/HT212874
https://support.apple.com/en-us/HT212867
https://support.apple.com/en-us/HT212876