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

CYBER GUIDANCE ISSUE 00100

ACTIVE ZERO-DAY EXPLOITS IN APPLE IOS

DATE ISSUED: 2nd February 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Apple has reported that three of their operating systems are known to be under active attack including iOS, iPadOS and tvOS. CVE-2021-1782, CVE-2021-1871, CVE-2021-1870.

BREAKDOWN

Attackers are actively exploiting the aforementioned operating systems in order to remotely execute code to gain elevated access privileges on effected devices. These vulnerabilities have appeared since the previous Apple security update and emergency patches have been released. CVE-2021-1782 exists in the OS kernel and the other two affect the WebKit browser engine. Apple has not released a great deal of information surrounding these vulnerabilities but are urging users to update as soon as possible.

REMEDIATION STEPS

- Apple devices should be updated immediately to the latest version.
- A full list of affected products and update instructions are available on the Apple website provided in the resources below.

REFERENCES & RESOURCES

CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/vulnerability-in-apple-ios-reportedly-being-actively-exploited/
Apple	https://support.apple.com/en-us/HT201222
Threatpost	https://threatpost.com/apple-patches-zero-days-ios-emergency-update/163374/