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

CYBER GUIDANCE ISSUE 00211

APPLE PATCHES BUG – NOW UNDER ACTIVE EXPLOIT

DATE ISSUED: 18th October 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Within hours of the release of a patch in the latest round of Apple updates, researchers published a Proof of Concept (PoC) for new Remote Code Execution (RCE) Zero-Day bug which is under active exploit affected devices using iOS 15.0.2 and iPadOS 15.0.2.

BREAKDOWN

While Apple has been focusing on upgrading performance for the latest version of their Operating Systems (OS), this is the first security release for the new version. Tracked as CVE-2021-30883, this vulnerability exists on the IOMobileFrameBuffer – a kernel extension that is used to assist developers in controlling how the memory of the device is used for screen display. If kernel level privileges are obtained, attackers would be able to execute arbitrary code and gain full control of the affected device. While Apple kept details of the security threat under wraps, a researcher has exposed the intricate details of the vulnerability in a report which has lead to attacker seizing the information and using it to perform attacks.

REMEDIATION STEPS

- Update the OS to the latest version to apply the security patches.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/apple-urgent-ios-updates-zero-day/175419/
PC Mag https://au.pcmag.com/security/90044/apple-patches-new-zero-day-ios-vulnerability-possibly-under-exploitation
Trend Micro https://www.trendmicro.com/vinfo/fr/security/news/mobile-safety/apple-promptly-releases-patch-after-zero-day-vulnerabilities-discovered