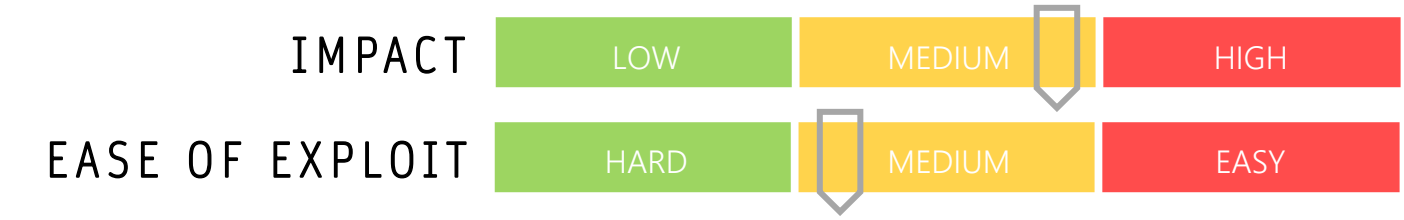
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00061

APPLE PATCHES ZERO-DAY FLAWS

DATE ISSUED: 10th November 2020



OVERVIEW

Three zero-day flaws, currently under exploit in the wild, which were identified by the Google Project Zero team have been patched in Apple's latest OS update which cover a total of 24 vulnerabilities.

CVE-2020-27930, CVE-2020-27950 and CVE-2020-27932.

BREAKDOWN

All three zero-day flaws affect all models including and upwards of the iPhone 6s, iPod touch 7th Gen, iPad Air 2 and iPad mini 4. The first is a memory corruption in the FontParser association with allowing the crafting of malicious fonts that may lead to arbitrary code execution. The second allows a malicious application to disclose kernel memory in the iOS kernel and is therefore a memory initialization flaw. The third improves state handling in the kernel to remedy what is describes as "a type of confusion issue" which would enable to execution of arbitrary code with kernel level privileges. These flaws were picked up by Google's Project Zero and Threat Analysis Group in relation to the Google Chrome patches issued last week. This brings the conflict between Google and Apple to a head, as Google claims these threats have been present for many months, even years with Apple refuting claims stating there was no evidence to support such claims.

REMEDIATION STEPS

- Ensure all Apple devices from the list above are running the latest version of iOS 14.2 and iPadOS 14.2
- Check for OS updates regularly on all devices.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/apple-patches-bugs-zero-days/161010/
Bleeping Computer	https://www.bleepingcomputer.com/news/security/apple-patches-three-actively-exploited-ios-zero-days/
Malwarebytes	https://blog.malwarebytes.com/exploits-and-vulnerabilities/2020/11/update-your-ios-now-apple-patches-3-zero-day-vulnerabilities/
We Live Security	https://www.welivesecurity.com/2020/11/06/apple-plugs-three-zero-day-holes-ios/
ZDNet	https://www.zdnet.com/article/apple-fixes-three-ios-zero-days-exploited-in-the-wild/