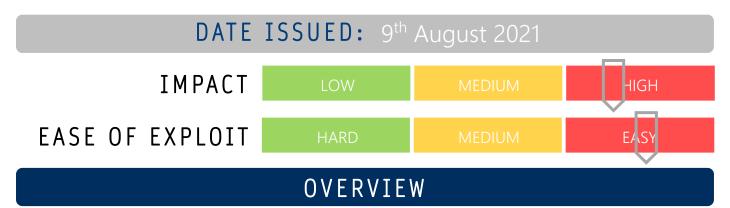




# CYBER GUIDANCE ISSUE 00182

### UPDATE APPLE DEVICES NOW



Critical vulnerabilities in Apple iPhones, iPads and Macs have been patched by apple to mitigate a memory corruption issue in the IOMobileFramebuffer kernel extension that is under known and active exploitation, tracked as CVE-2021-30807.

#### BREAKDOWN

Using kernel-level privileges, attackers are able to run arbitrary code on any of the affected devices to achieve full-takeover by exploiting this vulnerability. This is achieved by calling the external method 83 of *AppleCLCD/IOMFB* (which is *IOMobileFramebufferUserClient::s\_displayed\_fb\_surface*). Devices affected include Macs, iPhones 6 or later, all models of iPad Pro, iPad Air 2 and later, iPad 5<sup>th</sup> Gen or later, iPad mini 4 and later and iPod Touch 7<sup>th</sup> Generation.

## REMEDIATION STEPS

Update devices to iOS 14.7.1, iPadOS 14.7.1 ad macOS Bug Sur 11.5.1

#### REFERENCES & RESOURCES

CIS <a href="https://www.cisecurity.org/advisory/a-vulnerability-in-macos-big-sur-ios-and-ipados-could-allow-for-arbitrary-">https://www.cisecurity.org/advisory/a-vulnerability-in-macos-big-sur-ios-and-ipados-could-allow-for-arbitrary-</a>

code-execution/

Threatpost https://threatpost.com/apple-patches-actively-exploited-zero-day-in-ios-macos/168177/

 $\underline{\textbf{Bleeping Computer}} \ \underline{\textbf{https://www.bleepingcomputer.com/news/apple-fixes-zero-day-affecting-iphones-and-macs-exploited-in-plane} \ \underline{$ 

the-wild/