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

CYBER GUIDANCE ISSUE 00144

APPLE GATEKEEPER SECURITY BYPASS EXPLOITED

DATE ISSUED: 17th May 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Apple's primary security mechanism for code signing and verification is being bypassed using a vulnerability tracked as CVE-2021–30657 to drop malicious payloads by exploiting a policy subsystem bug. Apple has released patches to secure devices against the vulnerability.

BREAKDOWN

Malware known as Shlayer is being dropped by phishing campaigns and other means is able to run on Apple devices, bypassing all File Quarantine, Gatekeeper and Notarization requirements, even though the software is unsigned and unnotarized. With exploitation of this vulnerability believed to have begun in January this year, the malware has recently been repackaged to exploit CVE-2021–30657. The payload is being distributed by phishing and when the user opens the .dmg file and attempts to access the fake app inside there are no system generated alerts to inform the user of its malicious nature. MacOS identifies files in bundles, rather than single entities, which includes a list of properties which can be bundled in a certain way to circumvent the security features by an attacker.

A similar vulnerability CVE-2021-1810 is also able to bypass Gatekeeper and notarization checks but is not under known active exploitation.

REMEDIATION STEPS

- Update Apple Mac device OS to the latest version (macOS 11.3)

REFERENCES & RESOURCES

Threatpost https://threatpost.com/apple-patches-macos-bug-bypass-defenses/165611/
Apple https://support.apple.com/en-us/HT212325
ZDNet https://www.zdnet.com/article/apple-patches-macos-gatekeeper-bypass-vulnerability-exploited-in-the-wild