UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00151

APPLE MAC ZERO-DAY ALLOWS SNEAKY SCREENSHOTS

DATE ISSUED: 31st May 2021

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Apple has recently patched a vulnerability in macOS, tracked as CVE-2021-30713, discovered by security researchers where malware known as XCSSET has been able to take screen shots of users computers without their knowledge or permission.

BREAKDOWN

Bypassing the Transparency Consent and Control (TCC) framework which allows for collaboration over applications, the attacker is able to gain Full Disk Access, Screen Recording and other permissions. The default behaviour for this framework makes this possible without the users explicit consent. The malware is propagated by injecting XCSSET into Xcode developer projects. The malware hijacks the Safari web browser to inject JavaScript payloads and other malware to steal users information and capture their screen. The malwares suite was using two zero-day flaws - the Data Vault allowing it to bypass Mac security features and the WebKit used for Universal Cross Site Scripting (UXSS). A third zero-day bug also allowed for exploitation of the TCC using an AppleScript module “screen_sim.applescript” with the check “verifyCapturePermissions” to capture a screenshot from a list of installed apps to target apps that allow screen-sharing, verify the appID and craft a custom AppleScript application which is then injected as a donor application.

REMEDIATION STEPS

- Update Apple Mac computers to Big Sur 11.4 to apply the latest security patches.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/apple-patches-zero-day-flaw-in-macos-that-allows-for-sneaky-screenshots/166428/
Forbes	https://www.forbes.com/sites/thomasbrewster/2021/05/24/update-your-mac-now-nasty-hack-breaks-apple-security-to-take-sneaky-photos/
Jamf	https://www.jamf.com/blog/zero-day-tcc-bypass-discovered-in-xcsset-malware/