Hive Pro

THREAT ADVISORY

XCSSET malware exploits zero day TCC vulnerability in MacOS

TA202114

Threat Level Red

Publish Date – May 26, 2021

A zero-day vulnerability (CVE-2021-30713) in the latest macOS was exploited by XCSSET malware which allows an attacker to bypass the Transparency Consent and Control (TCC) framework and gives unauthorized access to the microphone, webcam, recording the screen, or even taking screenshots on infected Macs without prompting for user approval .The MITRE technique used by the adversary is T1222.

Vulnerability Details

CVE ID	Affected Versions	Affected CPEs	Vulnerability Name	CWE ID
CVE-2021-30713	macOS v11	cpe:2.3:o:apple:mac_os:11.0:*:*:*:*:*:*:*, cpe:2.3:o:apple:mac_os:11.1:*:*:*:*:*:*:*, cpe:2.3:o:apple:mac_os:11.2:*:*:*:*:*:*:*, cpe:2.3:o:apple:mac_os:11.3:*:*:*:*:*:*:*	Privilege escalation to bypass TCC framework	CWE-275

Indicators of Compromise

Type	Value
MD5	a23fbf615f7999a3089fb656ea29c8a7
SHA-1	60c7b8e84f5103f4597199f30bffcb79e4271d37
SHA-256	ba14cfe19a51a168813ee1d2bd2e57a8d2aeffa7721575772b6718114df778f3
Vhash	0767dfb013fffdb806d57f4360889c89
SSDEEP	192:7e9pNRGLdzBeZ5ahfdKcZXIWK5+o9lbOL0y8AU9To42t4EGUZJ34tSWBs:64zgah1KUXHAUhgt42E
TLSH	T1CFA23B729B0DD024C1BE8531BDFE87C39A50F0AA0F7473571B40D5B86FA4A98626678F
File type	Mach-O

Patch Link

https://support.apple.com/en-us/HT212529

References

https://support.apple.com/en-us/HT212529
https://threatpost.com/apple-patches-zero-day-flaw-in-macos-that-allows-for-sneaky-screenshots/166428/
https://www.ehackingnews.com/2021/05/apple-fixes-macos-zero-day.html
https://www.jamf.com/blog/zero-day-tcc-bypass-discovered-in-xcsset-malware/
https://www.darkreading.com/threat-intelligence/macos-zero-day-let-attackers-bypass-privacy-preferences/d/d-id/1341131
https://www.reviewgeek.com/85025/a-new-macos-update-patches-0-day-exploit-that-let-hackers-screenshot-on-your-mac/
https://vuldb.com/?id.175760