Hive Pro

THREAT ADVISORY

Old Gatekeeper bypass vulnerability in macOS exploited

TA202160

Threat Level AMBER

Publish Date – Dec 25, 2021

A gatekeeper bypass vulnerability exists in macOS Big Sur and has been assigned CVE-2021-30853. An attacker can exploit this issue by using a specially-crafted script-based application downloaded from the Internet. This allows an attacker to launch the application without displaying an alert while being automatically quarantined. The specially-crafted application uses a script starting with a shebang (!#) character and leaving the rest of the line empty, which tells the Unix shell to run the script without specifying a shell command interpreter. This bug bypasses not just Gatekeeper, but also File Quarantine, and macOS's recent notarization requirements.

It affects the macOS Big Sur versions up to 11.5.2 and has been fixed in version 11.6.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-30853	macOS Big Sur versions till 11.5	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	Apple macOS Big Sur security bypass	CWE-787

Patch Links

https://support.apple.com/en-us/HT212804

References

https://thehackernews.com/2021/12/expert-details-macos-bug-that-could-let.html
https://objective-see.com/blog/blog_0x6A.html
https://www.bleepingcomputer.com/news/apple/apple-fixes-macos-security-flaw-behind-gatekeeper-bypass/