INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

Action required: Apply patches to fix zero-day vulnerability in macOS

You're receiving this email because you're subscribed to UIT's public email list.

Note: *This message is also being sent to NotifyIT security channel subscribers via email and SMS. Please subscribe to NotifyIT if you wish to receive future IT security (and other IT incident) alerts.*

Actions to take

Mac users should prioritize macOS Big Sur system updates.

Summary

Apple has issued a patch for an actively exploited zero-day vulnerability on in macOS Big Sur versions before version 11.4 that allows XCSSET malware to surreptitiously move sensitive data — cryptocurrency addresses, credentials, and payment card information — from the Apple Store to the attacker's server. The vulnerability allows attackers to bypass privacy preferences and gain additional permissions. The available patch from Apple also fixes a number of other vulnerabilities.

Impact

The University of Utah's Information Security Office (ISO) is aware of the issue and is closely monitoring developments.

More information

- https://support.apple.com/en-us/HT212529
- https://www.helpnetsecurity.com/2021/05/25/cve-2021-30713-exploited/

If you have questions, your local IT support staff may be able to assist, or you may contact your respective central help desk: UIT Help Desk (801-581-4000, option 1) or the ITS Service Desk (801-587-6000).

Node 4 story idea? Email us: stratcomm@it.utah.edu

it.utah.edu

NotifyIT | Follow us on Twitter | IT Services Status | IT Service Portal