INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

Security flaw in Windows CryptoAPI (CVE-2020-0601)

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 subscribers via email.*

Summary

Microsoft recently issued an advisory about a spoofing vulnerability in the way Windows CryptoAPI validates elliptic-curve cryptography (ECC) certificates. If exploited, it could allow criminals to conduct man-in-the-middle attacks and decrypt confidential information on user connections to Windows 10 software.

Impact

The University of Utah's Information Security Office is aware of the issue and is closely monitoring developments. Microsoft has released security updates, as well as information about other ways to mitigate the risk.

Recommendations

Users should ensure their devices are up to date with currently-available patches.

More information

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601

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