INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

Security flaw in Microsoft Remote Desktop Services

Note: *This message is also being sent to NotifyIT security, infrastructure, and applications subscribers via email.*

Summary

Microsoft recently issued an advisory about a remote code execution vulnerability in Remote Desktop Services. If exploited, it could allow criminals to execute arbitrary code on the target system, enabling the attacker to install programs; view, change, or delete data; or create new accounts with full user rights.

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. Users also can disable Remote Desktop Services if they are not required.

More information

- https://support.microsoft.com/en-gb/help/4500705/customer-guidance-for-cve-2019-0708

If you have questions or need assistance, please contact your respective help desk: UIT Help Desk at 801-581-4000, option 1; ITS Service Desk at 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