On **Tuesday-Wednesday, June 20-21, 2023**, UIT will upgrade Windows domain controllers. The planned maintenance event will include a patch to mitigate IT security vulnerability [CVE-2022-38023](#) and will change how the Netlogon authentication protocol works.

This upgrade will cause older systems that run server message block version 1 (SMBv1), which Microsoft deprecated in 2013, and out-of-date network attached storage (NAS) to become inoperable. **Owners of potentially impacted systems should review and patch any dependent systems before June 20.**

Following the change, enforcement mode will be enabled on all Windows domain controllers and vulnerable connections from noncompliant devices will be blocked. At that time, system administrators will be unable to disable the update, but may temporarily move back to the compatibility mode setting until Microsoft removes it in July 2023.

Additional resources:

- [Netlogon RPC elevation of privilege vulnerability (CVE-2022-38023) update guide](#)
- [How to manage the Netlogon protocol changes related to CVE-2022-38023](#)
- [How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows](#)

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

Please visit the [University IT Services Status page](#) for information during this and future maintenance events.