NELSON HARDIMAN
HEALTHCARE LAWYERS

HIPAA Security Alert

The Office of Civil Rights (OCR) issued a Cyber Alert on September 22, 2020 regarding a vulnerability affecting Microsoft Server Operating Systems. According to the Cybersecurity and Infrastructure Security Agency (CISA), this vulnerability involves the Windows Netlogon Remote Protocol (CVE-2020-1472) and poses a significant security risk.

Earlier this month, exploit code for this vulnerability was publicly released and CISA assumes that it is in use by attackers to change a computer's active directory password, which could result in a denial of service and potentially allow an attacker to gain administrator privileges.

Q: Do I need to take action?

A: Given the significance of this vulnerability, CISA strongly recommends that both the public and the private sector take action to secure their networks. In light of OCR's Cyber Alert, covered entities and their business associates will need to review their systems immediately and if necessary, address the vulnerability for purposes of complying with the HIPAA Security Rule.

Q: What can I do to address this vulnerability?

A: Currently the only way to mitigate this vulnerability (other than removing affected domain controllers from the network) is to apply the August 11, 2020 security update to all Windows Servers with the domain controller role. If affected, domain controllers cannot be updated, and they should be removed from the network. Additionally, technical and/or management controls should be put into place to ensure newly provisioned or previously disconnected domain controller servers are updated before connecting to agency networks. Microsoft's guidance regarding managing the changes in Netlogon secure channel connections associated with CVE-202-1472 is available here.

Q: How do I know if I need to apply the August 11, 2020 security update?

A: The update is necessary for Windows Server 2019 (all editions), Windows Server 2016, Windows Server Version 1909 (all editions), Windows Server version 1903 (all editions), Windows Server version 1809 (Datacenter, Standard), Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 Service Pack. Organizations with sound patch management processes likely already installed the security update. Organizations should check with their IT Departments to see if the update was applied to all domain controllers and then confirm the update is complete by reviewing the domain controller audit logs for event ID 5829, which should identify any devices that have not been updated.

For questions regarding this client alert, please contact:
Lara Compton, Partner
lcompton@nelsonhardiman.com