TLP: WHITE
TO: All MS-ISAC and EI-ISAC Members and Partners

DATE: September 21, 2020


On September 18, the Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 20-04 (https://cyber.dhs.gov/ed/20-04/). This directive instructs entities of the need to ensure Windows servers are patched against the Netlogon elevation of privilege vulnerability (CVE-2020-1472) from the Microsoft August 2020 updates.

For background, on August 11, 2020, Microsoft released a software update to mitigate a critical vulnerability in Windows Server operating systems (CVE-2020-1472). The vulnerability in Microsoft Windows Netlogon Remote Protocol (MS-NRPC), a core authentication component of Active Directory, could allow an unauthenticated attacker with network access to a domain controller to completely compromise all Active Directory identity services.

Applying the update released on August 11 to domain controllers is currently the only mitigation to this vulnerability (aside from removing affected domain controllers from the network).

CISA has determined that this vulnerability poses an unacceptable risk to the Federal Civilian Executive Branch and requires an immediate and emergency action. This determination is based on the following:

- the availability of the exploit code in the wild increasing likelihood of any upatched domain controller being exploited;
- the widespread presence of the affected domain controllers across the federal enterprise;
- the high potential for a compromise of agency information systems;
- the grave impact of a successful compromise; and
- the continued presence of the vulnerability more than 30 days since the update was released.

This executive directive applies to all Federal government agencies as a requirement, but CISA strongly encourages all state and local government entities also protect themselves against this vulnerability.

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722
TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.