



Emergency Directive 20-04

Original Release Date: September 18, 2020

Applies to: All Federal Executive Branch Departments and Agencies, Except for the Department of Defense, Central Intelligence Agency, and Office of the Director of National Intelligence

FROM:

Christopher C. Krebs 
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

CC:

Russell T. Vought
Director, Office of Management and Budget

SUBJECT:

Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to “issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.” 44 U.S.C. § 3553(h)(1)–(2). Section 2205(3) of the Homeland Security Act of 2002, as amended, delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. 6 U.S.C. § 655(3). Federal agencies are required to comply with these directives. 44 U.S.C. § 3554 (a)(1)(B)(v). These directives do not apply to statutorily-defined “national security systems” nor to systems operated by the Department of Defense or the Intelligence Community. 44 U.S.C. § 3553(d), (e)(2), (e)(3), (h)(1)(B).

Background

On August 11, 2020, Microsoft released a software update to mitigate a critical vulnerability in Windows Server operating systems (CVE-2020-1472¹). 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:

¹ CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472>

- the availability of the exploit code in the wild increasing likelihood of any unpatched 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.

CISA requires that agencies immediately apply the Windows Server August 2020 security update to all domain controllers.

Required Actions

This emergency directive requires the following actions:

1. **Update all Windows Servers with the domain controller role** by 11:59 PM EDT, Monday, September 21, 2020,
 - a. **Apply the August 2020 Security Update** to all Windows Servers with the domain controller role. If affected domain controllers cannot be updated, ensure they are removed from the network.
 - b. By 11:59 PM EDT, Monday, September 21, 2020, **ensure technical and/or management controls are in place** to ensure newly provisioned or previously disconnected domain controller servers are updated before connecting to agency networks.

In addition to agencies using their vulnerability scanning tools for this task, CISA recommends that agencies use other means to confirm that the update has been properly deployed.

These requirements apply to Windows Servers with the Active Directory domain controller role in any information system, including an information system used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information.

2. **Report information to CISA**
 - a. By 11:59 PM EDT, Wednesday, September 23, 2020, **submit a completion report** using the provided template. Department-level Chief Information Officers (CIOs) or equivalents must submit completion reports attesting to CISA that the applicable update has been applied to all affected servers and provide assurance that newly provisioned or previously disconnected servers will be patched as required by this directive prior to network connection (per Action 1).

CISA Actions

- CISA will continue to work with our partners to monitor for active exploitation of this vulnerability.

- CISA will review and validate agency compliance and ensure that agencies participating in Continuous Diagnostic and Mitigation (CDM) program can leverage the support of their CDM system integrators (SIs) to assist with this effort, if needed. If agencies want to enlist the help of their CDM SIs, please notify your CDM Portfolio Team.
- CISA will provide additional guidance to agencies via the CISA website, through an emergency directive issuance coordination call, and through individual engagements upon request (via CyberDirectives@cisa.dhs.gov).
- Beginning October 1, 2020, the CISA Director will engage the CIOs and/or Senior Agency Officials for Risk Management (SAORM) of agencies that have not completed required actions, as appropriate and based on a risk-based approach.
- By October 5, 2020, CISA will provide a report to the Secretary of Homeland Security and the Director of Office of Management and Budget (OMB) identifying cross-agency status and outstanding issues.

Duration

This emergency directive remains in effect until all agencies have applied the August 2020 Security Update (or other superseding updates) or the directive is terminated through other appropriate action.

Additional Information

Visit <https://cyber.dhs.gov> or contact the following for:

- a. General information, assistance, and reporting – CyberDirectives@cisa.dhs.gov
- b. Reporting indications of potential compromise – Central@cisa.dhs.gov

Attachments:

1. Emergency Directive 20-04 Agency Report Template