**U.S. Department of Homeland Security**
Cybersecurity & Infrastructure Security Agency
*Office of the Director*
Washington, DC 20528

## Emergency Directive 20-03

Original Release Date: July 16, 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 (Acting), Office of Management and Budget

SUBJECT: **Mitigate Windows DNS Server Remote Code Execution Vulnerability from July 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 July 14, 2020, Microsoft released a software update to mitigate a critical vulnerability in Windows Server operating systems (CVE-2020-1350[1]). A remote code execution vulnerability exists in how Windows Server is configured to run the Domain Name System (DNS) Server role. If exploited, the vulnerability could allow an attacker to run arbitrary code in the context of the Local System Account. To exploit the vulnerability, an unauthenticated attacker sends malicious requests to a Windows DNS server.

The Cybersecurity and Infrastructure Security Agency (CISA) is unaware of active exploitation of this vulnerability, but assesses that the underlying vulnerabilities can be quickly reverse engineered from a publicly available patch. Aside from removing affected endpoints from the network, there are two known technical mitigations to this vulnerability:

1. a software update, and
2. a registry modification.

CISA has determined that this vulnerability poses unacceptable significant risk to the Federal Civilian Executive Branch and requires an immediate and emergency action. This determination is based on the likelihood of the vulnerability being exploited, the widespread use of the affected software across the

[1] CVE-2020-1350 | Windows DNS Server Remote Code Execution Vulnerability
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

Federal enterprise, the high potential for a compromise of agency information systems, and the grave impact of a successful compromise.

CISA requires that agencies apply the security update to all endpoints running Windows Server operating system as soon as possible. A registry modification workaround can help protect an affected Windows DNS server temporarily (until an update can be applied), and it can be implemented without requiring a restart of the server. The registry modification workaround will cause DNS servers to drop response packets that exceed the recommended value without error, and it is possible that some queries may not be answered. The registry modification workaround is compatible with the security update but should be removed once the update is applied to prevent potential future impact that could result from running a nonstandard configuration.

**Required Actions:**

This emergency directive requires the following actions:

1. **Update all endpoints running Windows Server operating systems.**
    a. By 2:00 pm EDT, Friday, July 17, 2020, **ensure the July 2020 Security Update or registry modification workaround is applied** to all Windows Servers running the DNS role.
    b. By 2:00 pm EDT, Friday, July 24, 2020, **ensure the July 2020 Security Update is applied** to all Windows Servers and, if necessary and applicable, the registry change workaround is removed.
    c. By 2:00 pm EDT, Friday, July 24, 2020, **ensure technical and/or management controls are in place** to ensure newly provisioned or previously disconnected servers are updated before connecting to agency networks.

    *CISA recommends agencies focus on updating Windows Servers running the DNS role first.*

    *These requirements apply to Windows Servers in any information system, including information systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information.*

    *In instances where servers cannot be updated within 7 business days, CISA advises agencies to consider removing them from their networks.*

2. **Report information to CISA**
    a. By 2:00 pm EST, Monday, July 20, 2020, **submit an initial status report** using the provided template. This report will include estimated status information related to the agency's current status and will identify constraints, support needs, and observed challenges.
    b. By 2:00 pm EST, Friday, July 24, 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 endpoints and providing 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 monitor and work with our partners to identify whether this vulnerability is actively being exploited.
- 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 August 13, 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 September 3, 2020, CISA will provide a report to the Secretary of Homeland Security and the Director of the 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 July 2020 Security Update 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

Attachment:

1. Emergency Directive 20-03 Agency Report Template