U.S. Department of Homeland Security
Washington, DC 20528

**Emergency Directive 20-02**

Original Release Date: January 14, 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 Vulnerabilities from January 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 January 14, 2020, Microsoft released a software patch to mitigate significant vulnerabilities in supported Windows operating systems. Among the vulnerabilities patched were weaknesses in how Windows validates Elliptic Curve Cryptography (ECC) certificates[1] and how Windows handles connection requests in the Remote Desktop Protocol (RDP) server and client.[2]

The vulnerability in ECC certificate validation affects Windows 10, Server 2016, and Server 2019. It bypasses the trust store, allowing unwanted or malicious software to masquerade as authentically signed

---

[1] CVE-2020-0601
[2] In particular, CVE-2020-0609, CVE-2020-0610, and CVE-2020-0611

by a trusted or trustworthy organization, which may deceive users or thwart malware detection methods like anti-virus. Additionally, a maliciously crafted certificate could be issued for a hostname that did not authorize it, and a browser that relies on Windows' CryptoAPI would not issue a warning, allowing an attacker to decrypt, modify, or inject data on user connections without detection.

Vulnerabilities in the Windows Remote Desktop client (affecting all supported versions of Windows, including Server) and RDP Gateway Server (affecting Server 2012, 2016, 2019) allow for remote code execution, where arbitrary code could be run freely. The server vulnerabilities do not require authentication or user interaction and can be exploited by a specially crafted request. The client vulnerability can be exploited by convincing a user to connect to a malicious server.

Though the Cybersecurity and Infrastructure Security Agency (CISA) is unaware of active exploitation of these vulnerabilities, once a patch has been publicly released, the underlying vulnerabilities can be reverse engineered to create an exploit. Aside from removing affected endpoints from the network, applying this patch is the only known technical mitigation to these vulnerabilities.

CISA has determined that these vulnerabilities pose an unacceptable risk to the Federal enterprise and require an immediate and emergency action. This determination is based on the likelihood of the vulnerabilities being weaponized, combined with the widespread use of the affected software across the Executive Branch and high potential for a compromise of integrity and confidentiality of agency information.

## Required Actions

This emergency directive requires the following actions:

1. **Patch all affected endpoints.**
    a. Within 10 business days (by 5:00pm EST, January 29, 2020), **ensure the January 2020 Security Updates patch is applied** to all affected endpoints on agency information systems.
    b. Within 10 business days (by 5:00pm EST, January 29, 2020), **ensure technical and/or management controls are in place** to ensure newly provisioned or previously disconnected endpoints are patched before connecting to agency networks.

    *CISA strongly recommends agencies initiate patching immediately, with a focus on patching the Windows 10 and Server 2016/2019 systems impacted by CVE-2020-0601. Agencies should prioritize patching mission critical systems and High Value Assets (HVAs), internet-accessible systems, and servers. Agencies should then apply the patch to the remaining endpoints. This applies to 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 these endpoints cannot be patched within 10 business days, CISA advises agencies to remove them from their networks.*

2. **Report information to CISA**

   a) Within 3 business days (by 5:00pm EST, January 17, 2020), **submit an initial status report** using the provided template. This report must include information related to the agency's current status and projected completion dates, and, if necessary, identified constraints, support needs, and observed challenges.

   b) Within 10 business days (by 5:00pm EST, January 29, 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 January 2020 Security Updates patch has been applied to all affected endpoints and providing assurance that newly provisioned or previously disconnected endpoints 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 these vulnerabilities are being exploited.
- CISA will provide additional guidance to agencies on the CISA website, through an emergency directive issuance coordination call, and through individual engagements upon request (via CyberDirectives@hq.dhs.gov).
- CISA will review and validate agency compliance and ensure that agencies participating in CDM can leverage the support of their system integrators to assist with this effort, if needed.
- Beginning February 3, 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.
- By February 14, 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 replaced by a subsequent binding operational directive or terminated through other appropriate action.

## Additional Information

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

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

Attachment:

1. Emergency Directive 20-02 Agency Report Template
2. CISA Activity Alert 20-014A