

The NSA issued an urgent warning about a critical vulnerability appearing in Windows servers

This is a vulnerability that exists in the cryptographic authentication scheme used by the Netlogon Remote Protocol.

The US government is facing a huge problem related to server security. The US Department of Homeland Security (CISA) Cybersecurity and Infrastructure Agency (CISA) has issued an emergency directive calling for government agencies to install patches for 'critical' Windows Server security vulnerabilities. 'is called Zerologon.

Zerologon is a vulnerability that exists in the cryptographic authentication scheme used by the Netlogon Remote Protocol. If abused, it can pave the way for an attacker to impersonate any computer, including the Domain Controller itself, and then gain access to Active Directory services on the network without having to. log in, as well as make remote procedure calls.

More specifically, by forging an authentication token for a particular Netlogon function, an attacker can call a function that sets the Domain Controller's password to a known value. They can then use this new password to gain control of the Domain Controller and steal the domain administrator's credentials.

CISA is currently warning of serious consequences, the availability of 'in the wild' exploits, and the sheer popularity of vulnerable Windows servers acting as Domain Controllers. Basically, Zerologon affects systems running Windows Server 2008 R2 or higher, including recent systems using Windows 10 based Server editions.

Emergency directive 20-04 has been issued by CISA, instructing federal civil authorities to apply the August 2020 Windows Servers security update (August 2020 security update - CVE-2020-1472) Microsoft is for all Domain Controllers. Patch installation must be done in September.

Home

- 20-04 - Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday
- Background
- Required Actions
- CISA Actions

20-03 - Mitigate Windows DNS Server Vulnerability from July 2020 Patch Tuesday

20-02 - Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday

20-01 - Vulnerability Disclosure Policies

19-02 - Vulnerability Remediation

Emergency Directive 20-04

September 18, 2020

Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's [Emergency Directive 20-04](#), "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\(h\)\(2\)-\(2\)](#)

Section 2205(j) 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\(j\)](#).

Federal agencies are required to comply with these directives. [44 U.S.C. § 3554 \(a\)\(2\)\(B\)\(i\)](#)

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\(d\), \(e\)\(2\), \(e\)\(3\), \(b\)\(1\)\(B\)](#).

Although the CISA warning is issued to US government agencies, it is essentially the same warning for private companies that depend on Windows servers and Active Directory.

If the intruder successfully exploits this vulnerability, they will have the right to control the network effectively, thereby spreading malware, stealing data or causing serious problems. Many companies have suffered huge damage from malware this year, and that trend may continue if they fail to protect themselves against risks like Zerologon in time.

You finished reading the article "**The NSA issued an urgent warning about a critical vulnerability appearing in Windows servers**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.