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.

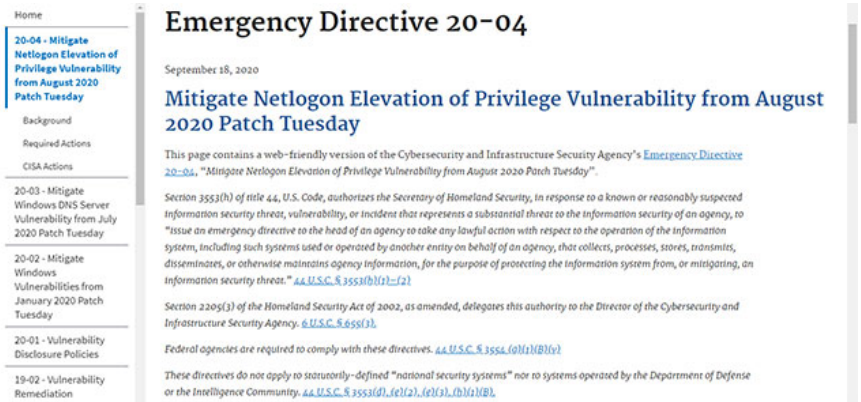
The US government is facing a huge problem related to server security. The US Department of Homeland Security (CISA) Cybersecurity and Infrastructure Agency (CISA) has issued an emergency directive calling for government agencies to install patches for 'critical' Windows Server security vulnerabilities.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



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.