The CredSSP vulnerability in the RDP protocol affects all versions of Windows

A serious vulnerability just found on the CredSSP protocol affects all versions of Windows, allowing attackers to exploit RDP and WinRM to steal data or run malicious code.

A serious vulnerability has just been found on the Credential Security Support Provider (CredSSP) protocol that affects all Windows versions, allowing attackers to exploit RDP and WinRM to steal data or run malicious code.

CredSSP protocol is used by RDP (Remote Desktop Protocol) and WinRM (Windows Remote Management), is responsible for forwarding encrypted authentication information from Windows client to server for remote authentication.

Discovered by researchers at Preempt Secutiry, this vulnerability (CVE-2018-0886) is a logical error in CredSSP, which allows an intermediary to use WiFi or physically connect to the network to steal authentic data and Attack Remote Procedure Call.

'The data theft attacker from the user can run the command with admin rights. This is especially important when controlling domain names, when most Remote Procedure Call (RPC / DCE) are turned on automatically, 'said Yaron Zinar, a researcher in Preempt.

Because RDP is the most popular application for remote login and most business customers use RDP, most networks are at risk because of this error.

The problem was reported to Microsoft by Preempt last August, but it was not until Patch Tuesday that it lasted nearly seven months - they patched the vulnerability.

Researchers also warn that patching alone is not enough to prevent attacks, IT professionals should change some of the necessary configurations. Blocking related application ports including RDP or DCE / RPC also helps to reduce but this type of attack can be done in many ways with other protocols.

Therefore, above all, it is advisable to limit the use of the highest possible account. March Patch Patch also patched other software such as Microsoft IE, Edge, Windows OS, Office, PowerShell, Core ChakraCore and Adobe Flash.

See more:

1. Top 12 most dangerous backdoor in computer history
2. Secure Terminal Services of Windows Server 2008
3. Access Windows Remote Desktop via Internet