Immediately fix critical vulnerabilities in Windows NTLM security protocol

Researchers on Firewall Preempt behavior have discovered two new vulnerabilities in Windows NTLM security protocols. Let's see what those holes are and how serious it is!

Microsoft has released a security patch for a particularly serious security vulnerability that affects all versions of Windows operating systems for businesses released since 2007.

Researchers on Firewall Preempt behavior have discovered two new vulnerabilities in Windows NTLM security protocols, both of which allow attackers to create an administrator account with a new domain name (domain) and control the entire domain.

See details at: https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/f2b16606-4945-e711-80dc-000d3a32fc99

NT LAN Manager (NTLM) is an old authentication protocol used on networks - including Windows systems and standalone systems.

Although NTLM has been replaced with Kerberos in Windows 2000, it still provides better security for systems on the same network, which is still supported by Microsoft and widely used.

The first vulnerability related to the **Lightweight Directory Access Protocol (LDAP)** is not protected on NTLM and the second vulnerability affects the **Restricted-Admin Remote Desktop Protocol (RDP) mode** . These vulnerabilities make it easier for attackers to perform LDAP operations such as updating domain objects instead of NTLM users, accessing unauthorized information and allowing connection to remote computers without a need. password.

In a blog post, Yaron Zinar said: " *To realize how serious the problem is, we must know all Windows protocols using the Windows Authentication API (SSPI) to allow downgrade. authenticated to NTLM* . "

According to Preempt researchers, RDP Restricted-Admin allows NTLM downgrade authentication systems. This means that attacks performed with NTLM such as relaying authentication information and password breaks can also be performed against RDP Restricted-Admin.

When combined with an LDAP vulnerability, an attacker can create a fake domain admin account when the admin connects to RDP Restricted-Admin and controls the entire domain.

Microsoft said an attacker could exploit this vulnerability by running a special application to send malicious traffic to the domain controller. We can update these vulnerabilities by combining improvements to authentication protocols designed to minimize attacks.

Therefore, system administrators are encouraged to patch vulnerable servers by activating NT LAN Manager as soon as possible.

Besides leaking this NTLM, Microsoft has also released patches for 55 security holes, including 19 important products including Edge, Internet Explorer, Windows, Office, Office Services, Web Apps, and .NET Framework. and Exchange Server .

Windows users are advised to install the latest update immediately to protect themselves in ongoing attacks.