How to mitigate PetitPotam NTLM Relay Attack

calcomsoftware.com/how-to-mitigate-petitpotam-ntlm-relay-attack

March 27, 2022

The latest Windows versions are compatible with NTLM and default NTLM implementation necessitates Active Directory. Microsoft has shared instructions on mitigating PetitPotam a type of NTLM relay attack that is used against Windows domain servers or controllers. Microsoft has referred to it as the 'classic' NTLM (ADV210003) relay attack allowing an attacker to take over domain controller or other Windows servers.

Signs of Petitpotam Vulnerability

As an organization, you can be vulnerable to the threat or attack in cases where the servers featuring Active Directory Certificate Servers have not been configured with proper protections. PetitPotam is a vulnerability using NTLM's remote authentication protocol – EFSRPC, enabling attackers to initiate an NTLM relay attack and get control over your Windows domain.

An attacker sends a connection request with a Domain Controller using EFSPRC and pushes the usage of NTLM (rather than Kerberos or safer authentication alternatives). Once this NTLM authentication is done, the attacker initiates an NTLM relay to steal the hashed password.

The IIS servers, installed over Domain Controllers, used for certificate service web enrollment, are the major target of the attackers. Upon acquiring the domain credentials, he can easily break the web enrollment, steal the certificate and get domain authority.

If you don’t want to be a victim of this vulnerability, restricting or limiting the NTLM incoming traffic is a better choice rather than disabling NTLM in the whole network.

How to Mitigate the Risk?

Microsoft reveals that administrators can look forward to preventing this attack by disabling NTLM authentication on the Windows domain controller. The company reveals that it is the simplest way to ensure mitigation of the risks.
Admins can achieve the same by following the guidelines specified in the documentation of Network Security -Restrict NTLM -NTLM (KB5005413) authentication in the domain.

If NTLM cannot be disabled due to reasons related to compatibility, admins can be directed towards disabling NTLM on any of the given AD CS Servers in the given domain. It can be achieved by

- Opening the group policy of Network Security
- Restrict NTLM – Incoming NTLM traffic

As per Microsoft, you can configure the GPO. You can then open Group Policy and advance to Computer Configuration.

Then, head to Windows Settings -> Security Settings -> Local Policies -> Security Options

You can then set 'Network Security -Restrict NTLM -Incoming NTLM Traffic' to the option 'Deny All Accounts' or 'Deny All Domain Accounts

Admins can also think of disabling NTLM for Internet Information Services on AD CS servers in the domain executing Certificate Enrollment Web Service or Certificate Authority Web Enrollment.

Microsoft has recently announced the release of the **SMB NTLM Authentication Rate Limiter** on their vNext server that has a default 2 second delay between each failed NTLM-based authentication slowing down the bad actors when attempting brute force password identification.

Conclusion

Complex environments often make hardening a difficult process, necessitating hours of work and resources. Moreover, hardening usually leads to downtime anyhow. More than 60% of IT teams reported they experience downtime during infrastructure hardening.

These types of attacks emphasizes the need to stop using old and vulnerable services such as NTLM. Since it is a complex task for organizations with a large infrastructure, it also emphasizes the need for hardening automation tools. CalCom's Hardening Solution (CHS) automates server hardening. CHS will report to you where NTLM is being used and where you can disable NTLM. It will also enforce your policy in the production environment making sure everything is configured correctly. Finally, it will monitor and fix any configuration drifts to make sure you remain comp