Microsoft Releases Guidance for Mitigating PetitPotam NTLM Relay Attacks

Vulnerability Bulletins | Jul 27, 2021, 02:25 PM

Microsoft has publicly released an alert, KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS), to address a NTLM Relay Attack, designated PetitPotam. The alert is supplied with active mitigation strategies and recommendations for organizations potentially affected by the PetitPotam relay attack.

PetitPotam is a novel attack method that can be used to conduct a New Technology LAN Manager (NTLM) relay attack upon targeted organizations. The attack uses the Microsoft Encrypting File System Remote Protocol (EFSRPC) to force a device to authenticate to a remote NTLM relay directly controlled by a threat actor. Once the device authenticates to the malicious NTLM server, a threat actor can steal hashes and certificates that can be used to assume the identity of the device and its privileges. This identity theft can be used independently or used in further attacks upon targeted organizations.

Researchers have released a proof-of-concept script for the PetitPotam technique on GitHub that can be used to force a domain controller to authenticate against a remote NTLM relay under an attacker's control using the MS-EFSRPC API. This proof-of-concept release has a significant impact upon the development time for threat actors, as this code could be utilized to quickly weaponize tools and techniques for attackers in future campaigns.

Recommendations:
Microsoft recommends disabling NTLM where it is not necessary in your environment.

To prevent NTLM Relay Attacks on networks where NTLM is enabled, domain administrators must ensure that services that permit NTLM authentication make use of protections such as Extended Protection for Authentication (EPA) or signing features such as SMB signing.

The Cybersecurity and Infrastructure Security Agency (CISA) is now encouraging users and administrators to review KB5005413 and to apply the necessary mitigations.

Sources:
Microsoft KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS)
Bleeping Computer: Microsoft Shares Mitigations for New PetitPotam NTLM Relay Attack
Threatpost: Microsoft Rushes Fix for 'PetitPotam' Attack PoC
ZDnet: Microsoft: Here's How to Shield Your Windows Servers Against This Credential Stealing Attack

Sophos: Windows “PetitPotam” Network Attack – How to Protect Against It

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Reference(s)

SophosMicrosoftBleeping ComputerZDNetThreat Post