UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00178

PETITPOTAM CREDENTIAL STEALING ATTACKS

DATE ISSUED: 3rd August 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A Proof of Concept (PoC) for Windows NT LAN Manager (NTLM) exploit has been published revealing that remote Windows systems can be forced to reveal password hashes, which can then be cracked in a Man-in-the-Middle (MITM) style attack over the Internet.

BREAKDOWN

PetitPotam exploits the Encrypting File System Remote Protocol (MS-EFSRPC) which allows remote access to encrypted data stores with enforceable access control policies. Executing a manipulator-MITM attack, followed by the use of Server Message Block (SMB) to request access to a system, this induces authentication detail sharing via NTLM. The attacker is then able to intercept the password hashes to crack offline, due to the weak nature of this protocol that is still in use. PetitPotam can be used as a preliminary attack and daisy-chained with attacks to then exploit Windows Active Directory Certificate Services (AD CS) as demonstrated in the PoC. Servers are vulnerable if they are using NTLM or AD CS with the services Certificate Authority Web Enrolment and Certificate Enrolment Web Services.

REMEDIATION STEPS

- Disable NTLM authentication on Windows Domain Controllers.
- Use the Extended Protection for Authentication (EPA) feature and AD CS.
- Alternatively, if NTLM cannot be disable, make sure EPA and other signing features (SMB signing) are enabled and research other methods to prevent NTLM Relay Attacks.

REFERENCES & RESOURCES

ZDNet https://www.zdnet.com/article/microsoft-heres-how-to-shield-your-windows-servers-against-this-credential-stealing-attack
Threatpost https://threatpost.com/microsoft-petitpotam-poc/168163/
Microsoft https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429
The Record https://therecord.media/new-petitpotam-attack-forces-windows-hosts-to-share-their-password-hashes/