NTLM Keeps Haunting Microsoft

crowdstrike.com/blog/ntlm-keeps-haunting-microsoft/

Yaron Zinar

August 26, 2021

Two severe Windows NT LAN Manager (NTLM) vulnerabilities were recently disclosed: PetitPotam and AD-CS relay (specifically ESC8). These vulnerabilities follow a pattern of NTLM issues in recent years. These vulnerabilities are bad on their own, but their combination can be devastating: If a network is not protected, the combination can allow an attacker with network access alone to achieve full domain admin privileges.

This blog post skips some of the deep technical details of these two vulnerabilities (there are plenty of great resources online) and instead provides a wider and richer context for recent attacks and similar issues that lurk in Active Directory (AD) environments.

Summary

PetitPotam is a coerced authentication that acts as an enabler for NTLM relay. Its key strength compared to Print Spooler coerced authentication is that it works *unauthenticated* (an attacker only needs network access). AD-CS relay (ESC8) is the more critical issue since the AD-CS default configuration does not protect from NTLM relay. Relaying privileged authentication to an AD-CS server results in full domain takeover. Microsoft partially addressed one of the issues related to PetitPotam on Aug. 10, 2021, as discussed in our August 2021 Patch Tuesday blog. We have not performed an independent analysis of the patch, but researchers have stated it does not solve all of the authentication issues abused by PetitPotam unless additional controls are also implemented. Microsoft has not fixed the AD-CS relay by default but has issued an advisory to guide customers on how to enable protection.

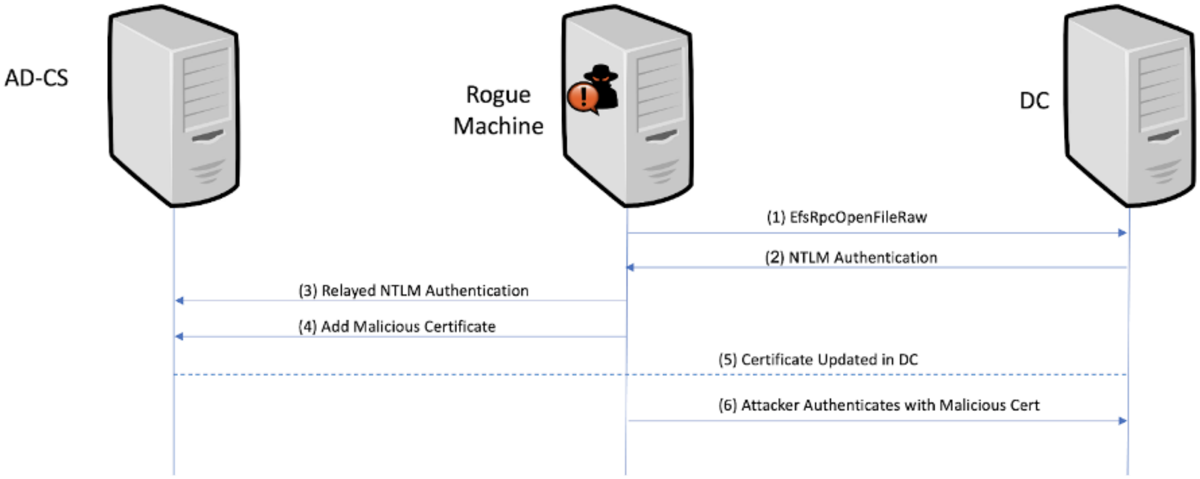

AD-CS
Rogue Machine
DC
(1) EfsRpcOpenFileRaw
(2) NTLM Authentication
(3) Relayed NTLM Authentication
(4) Add Malicious Certificate
(5) Certificate Updated in DC
(6) Attacker Authenticates with Malicious Cert

Figure 1. Combined PetitPotam and ESC8 attack flow

Coerced Authentication

PetitPotam is a coerced authentication vulnerability. Coerced authentication is a procedure where the attackers trigger a remote authentication to a compromised machine. When the attackers capture the network login on the compromised machine, they can use this authentication to perform:

1. **Password Cracking**: When the attackers coerce a user account authentication and the attacked client supports NTLM, attackers can use the captured NTLM authentication to perform password cracking. When NTLMv1 is supported (less common), attackers can use the weak cryptography to extract a password hash more easily. The authentication coercion techniques described below trigger computer account authentication and thus are not susceptible to password-cracking attacks since computer accounts have strong randomly generated passwords that rotate on a monthly basis.

2. **Credentials Relay**: Credentials relay has two flavors:
    1. **NTLM Relay:** This is the more common attack. There is plenty of material out there on NTLM Relay — for a deeper overview, start with the introduction to server signing attacks and EPA attacks. In my experience, Microsoft has treated NTLM relay attacks as actual vulnerabilities that required patching only if there was no safe configuration (for example, with CVE-2021-1678). However, if a safe configuration was available, Microsoft typically published an advisory while keeping the insecure defaults, possibly out of concern that changing the default configuration may have resulted in breaking various applications. This means that in many cases, defenders can be left with insecure defaults.
    2. **Kerberos Relay**: In most cases, attackers cannot relay Kerberos authentications. However, if attackers are able to compromise an account with sufficient delegation privileges, they can perform Kerberos authentications on behalf of other users. A recent interesting vulnerability discovered in this space is the Bronze Bit attack.

Two well known authentication coercion attacks are the “Printer Bug” and PetitPotam:

The “Printer Bug”

An important issue that exists in the print spooler service is the “Printer Bug,” which is an authentication coercion mechanism. The issue was reported by Lee Christensen from SpectreOps in 2018, and initially Microsoft did not fix it completely, but has removed the coerced authentication in Windows Server 2019. Similar to the new PetitPotam attack, this attack enables the attackers to trigger authentication by a remote host’s computer account. If the remote machine is privileged (e.g., a domain controller), that authentication can be relayed and the computer account privileges are used.

PetitPotam (MS-EFSRPC)

PetitPotam is an authentication coercion mechanism that takes advantage of MS-EFSRPC (interface c681d488-d850-11d0-8c52-00c04fd90f7e) via EfsRpcOpenFileRaw function. PetitPotam has two notable advantages:

1. The EfsRpcOpenFileRaw function works unauthenticated. This means any attacker with network access alone could potentially exploit this issue.
2. PetitPotam is a more recent coerced and remains viable on all Windows versions to date.

Missing NTLM Relay Protections

The second vulnerability is a classical NTLM relay attack. NTLM relay attacks are a very old attack technique. In general, Microsoft offers two main mitigations to protect from NTLM relay:

- Server Signing (SMB Signing / LDAP Signing)
- Channel Bindings (EPA = Extended Protection for Authentication).

Some of these protections are enabled by default (e.g., SMB Signing on Domain Controllers), and some require special configuration by IT administrators (e.g., EPA for LDAP over TLS).

AD-CS Relay (ESC8)

Will Schroeder and Lee Christensen have published Certified Pre-Owned, a white paper detailing many attacks on AD certificate-based authentication. Along with the white paper, they have released a defensive audit tool allowing IT administrators and security professionals to find existing issues in their network. I want to focus on one specific issue: ESC8. ESC8 is the discovery that the AD certificate server (AD-CS) by default does not enforce EPA on incoming connections. This means that if attackers are able to capture a privileged enough authentication request, it can be relayed to the AD-CS server and allow the attackers to create a certificate for the relayed account and then authenticate as that user account. Since the user is privileged (e.g., the DC account), the attacker now has full domain privileges.

LDAPS Relay (CVE-2017-8563)

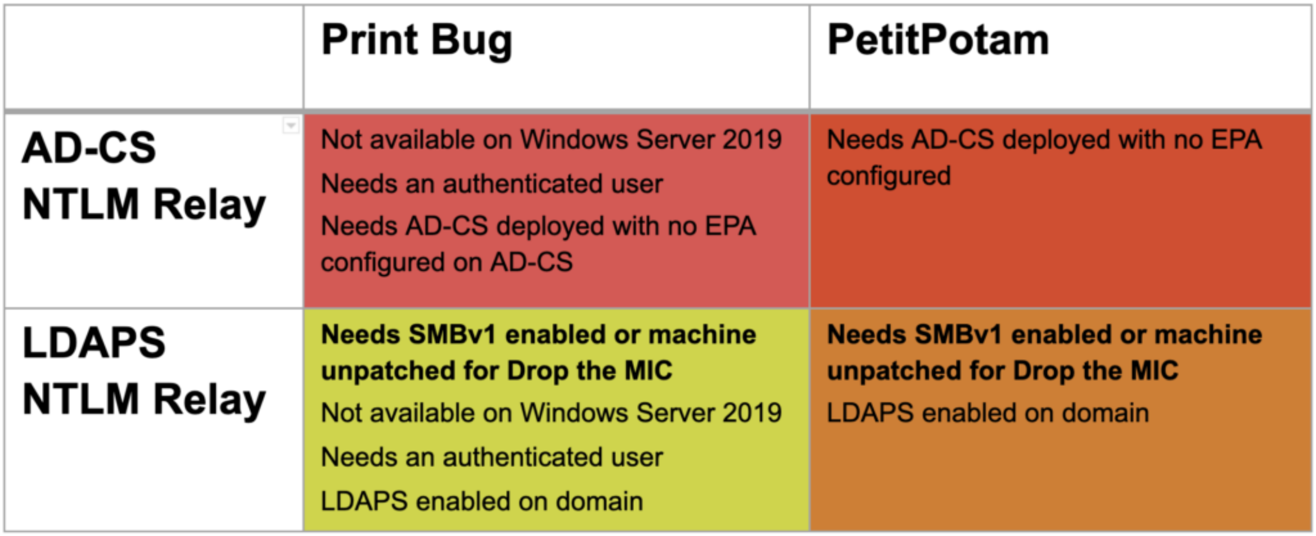
Another important attack surface for NTLM relay attacks is LDAP. The LDAP protocol allows not only querying the directory data, but also changing directory data such as adding users, adding users to security groups, creating new computers and more. LDAP has two main supported access method:

1. **LDAP over port 389:** This is the regular LDAP port. LDAP is protected there by server signing, which is not turned on by default.
2. **LDAPS – LDAP over TLS (port 636):** This is the same LDAP protocol protected by TLS. Prior to 2017, LDAPS was not protected from NTLM relay at all (CVE-2017-8563). To protect LDAPS, Microsoft introduced channel bindings, which are essentially EPA protection for LDAPS. Unfortunately, Microsoft has not enabled this protection by default, and thus many networks are still unprotected today.

As you can see, LDAP protections are not enabled by default. **We see that for more than 90% of CrowdStrike Identity Protection customers, these configurations are not in a secure manner.** This is partially mitigated since when the client sets the signing flag in the NTLM message, LDAP/S relay is mitigated (more details in the wonderful blog by Pixis). This makes LDAP relay a slightly less common relay target. However, if an NTLM client supports SMBv1 and/or the NTLM server is vulnerable to Drop the MIC (see more in our 2019 blog), LDAP/S relay can still occur.

Attack Summary

The following table summarizes attack feasibility for the described methods.



	Print Bug	PetitPotam
AD-CS NTLM Relay	Not available on Windows Server 2019 Needs an authenticated user Needs AD-CS deployed with no EPA configured on AD-CS	Needs AD-CS deployed with no EPA configured
LDAPS NTLM Relay	**Needs SMBv1 enabled or machine unpatched for Drop the MIC** Not available on Windows Server 2019 Needs an authenticated user LDAPS enabled on domain	**Needs SMBv1 enabled or machine unpatched for Drop the MIC** LDAPS enabled on domain

Figure 2. Availability of recent NTLM relay attacks

How to Protect Your Network

In order to protect your network, we suggest following these steps:

Set Secure Configuration

The following secure configurations are required:

1. **Enforce SMB Server Signing**. SMB signing is required by default on domain controllers, which is good. However, not all other workstations and servers in the network are protected by default. An important note is that by default relaying SMBv2->SMBv2 (a very important scenario) is possible.
2. **Enforce EPA and Channel Binding on all critical servers**. This is extremely important since in practically all cases, EPA protection **is not enabled** by default. Typically, EPA protection can be *enabled* or *required*. While setting EPA=*required* offers better protection, setting EPA=*enabled* will block most relay attacks.
3. **Disable NTLM**. Even though steps 1 and 2 can almost completely mitigate NTLM relay (aside from zero days), NTLM has many issues in addition to NTLM relay, and it is advisable to completely stop using NTLM. Turning off NTLM, however, is a complex IT project that requires planning and time. The first and most critical step is understanding which systems in your network are still using NTLM and why. This step has proven to be non-trivial for many organizations. Once you have your network mapped, you can start the migration process.

Patching

In some cases, there are no secure defaults, so make sure your environment is patched against the following relay vulnerabilities:

1. **Drop the MIC**: CVE-2019-1040 can enable attackers to perform successful LDAP relay attacks. While this is an old vulnerability, make sure you are fully patched against the vulnerability.
2. **DCE/RPC Relay**: Apply patched for CVE-2021-1678 and CVE-2020-1113.
3. **PetitPotam**: As we have suggested, the patch probably does not solve the coerced authentication issue entirely. However, it is recommended to install a patch for CVE-2021-36942.

Disable Unnecessary Services

1. Disable the Printer Spooler service on all critical servers.
2. MS-EFSRPC: Either disable the service entirely or follow the Microsoft advisory and enforce EPA and AD-CS authentications.

Audit Your Environment

It is obvious that keeping track of all configurations (NTLM, AD-CS, enabled services, EPA, signing requirements, patch status) is almost impossible manually. In order to make sure you are fully protected, an automated audit solution is required.

Falcon Spotlight™ customers can quickly see if their environments are vulnerable using the PrintNightmare dashboard. For those who wish to trial Spotlight for free, please see the CrowdStrike Store.

Additional Resources

- *Learn more by reading the white paper, "The Security Risk of NTLM."*
- *Visit the CrowdStrike Falcon Identity Protection solutions webpage.*
- *Request a demo of CrowdStrike Falcon Zero Trust or Falcon Identity Threat Detection products.*
- *Learn more about the CrowdStrike Falcon® platform by visiting the product webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*
- *Learn more on how Falcon Spotlight can help you discover and manage vulnerabilities in your environments.*