PetitPotam Attack Chain Can Compromise Windows Domains Running AD CS | Rapid7 Blog

By Rapid7

Published: 2021-08-03 · Archived: 2026-04-05 14:03:51 UTC

The PetitPotam attack vector was assigned CVE-2021-36942 and patched on August 10, 2021. See the Updates section at the end of this post for more information.

Late last month (July 2021), security researcher Topotam published a proof-of-concept (PoC) implementation of a novel NTLM relay attack christened “PetitPotam.” The technique used in the PoC allows a remote, **unauthenticated** attacker to completely take over a Windows domain with the Active Directory Certificate Service (AD CS) running — including domain controllers. Rapid7 researchers have tested public proof-of-concept code against a Windows domain controller setup and confirmed exploitability. One of our senior researchers summed it up with: "This attack is too easy."

PetitPotam works by abusing Microsoft’s Encrypting File System Remote Protocol (MS-EFSRPC) to trick one Windows host into authenticating to another over LSARPC on TCP port 445. Successful exploitation means that the target server will perform NTLM authentication to an arbitrary server, allowing an attacker who is able to leverage the technique to do... pretty much anything they want with a Windows domain (e.g., deploy ransomware, create nefarious new group policies, and so on). The folks over at SANS ISC have a great write-up here.

According to Microsoft’s ADV210003 advisory, Windows users are potentially vulnerable to this attack if they are using Active Directory Certificate Services (AD CS) with any of the following services:

- Certificate Authority Web Enrollment
- Certificate Enrollment Web Service

NTLM relay attacks aren’t new—they’ve been around for decades. However, a few things make PetitPotam and its variants of higher interest than your more run-of-the-mill NTLM relay attack. As noted above, remote attackers don’t need credentials to make this thing work, but more importantly, there’s no user interaction required to coerce a target domain controller to authenticate to a threat actor’s server. Not only is this easier to do — it’s faster (though admittedly, well-known tools like Mimikatz are also extremely effective for gathering domain administrator-level service accounts). PetitPotam is the latest attack vector to underscore the fundamental fragility of the Active Directory privilege model.

Microsoft released an advisory with a series of updates in response to community concern about the attack — which, as they point out, is “a classic NTLM relay attack” that abuses intended functionality. Users concerned about the PetitPotam attack should review Microsoft’s guidance on mitigating NTLM relay attacks against Active Directory Certificate Services in KB500413. Since it looks like Microsoft will not issue an official fix for this

vector, community researchers have added PetitPotam to a running list of “won’t fix” exploitable conditions in Microsoft products.

The PetitPotam PoC is already popular with red teams and community researchers. We expect that interest to increase as Black Hat brings further scrutiny to Active Directory Certificate Services attack surface area.

Mitigation Guidance

A patch that mitigates this attack chain is available as of August 10, 2021. Windows administrators should apply the August 10, 2021 patch for CVE-2021-36942 as soon as possible, prioritizing domain controllers, and then follow the guidance below as specified in KB5005413.

In general, to prevent NTLM relay attacks on networks with NTLM enabled, domain administrators should ensure that services that permit NTLM authentication make use of protections such as Extended Protection for Authentication (EPA) coupled with “Require SSL” for affected virtual sites, or signing features such as SMB signing. Implementing “Require SSL” is a critical step: Without it, EPA is ineffective.

As an NTLM relay attack, PetitPotam takes advantage of servers on which Active Directory Certificate Services (AD CS) is not configured with the protections mentioned above. Microsoft’s KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS) emphasizes that the primary mitigation for PetitPotam consists of three configuration changes (and an IIS restart). In addition to primary mitigations, Microsoft also recommends disabling NTLM authentication where possible, starting with domain controllers.

In this order, KB5005413 recommends:

- Disabling NTLM Authentication on Windows domain controllers. Documentation on doing this can be found here.
- Disabling NTLM on any AD CS Servers in your domain using the group policy Network security: Restrict NTLM: Incoming NTLM traffic. For step-by-step directions, see KB5005413.
- Disabling NTLM for Internet Information Services (IIS) on AD CS Servers in your domain running the "Certificate Authority Web Enrollment" or "Certificate Enrollment Web Service" services.

While not included in Microsoft’s official guidance, community researchers have tested using NETSH RPC filtering to block PetitPotam attacks with apparent success. Rapid7 research teams have not verified this behavior, but it may be an option for blocking the attack vector without negatively impacting local EFS functionality.

The majority of the guidance on PetitPotam, including in Microsoft's advisory, focuses on domains on which Active Directory Certificate Services are running. Unfortunately, even users *not* running AD CS can be vulnerable to PetitPotam. We've written a little about why below.

PetitPotam is a means by which to trigger an authentication attempt from a target Windows system to an attacker-controlled system. This authentication attempt can then be captured and used for offline brute forcing, or more commonly relayed to authenticate to another target service. When Microsoft released MS08-068, it removed the ability to relay an authentication attempt back to the same target using the same service. In other words, an incoming SMB authentication attempt to an attacker cannot be relayed back to the target to authenticate to SMB and create a service to execute code (like PSexec does).

The attack identified as ESC8 and documented in the whitepaper Certified Pre-Owned describes a scenario in which an attacker can perform an NTLM relay attack to the AD CS HTTP endpoint to make authenticated API calls. The original work suggests using the MS-RPRN methods RpcRemoteFindFirstPrinterChangeNotification methods. However, these methods require that the connection be authenticated.

The PetitPotam technique is ideally suited to substitute the MS-RPRN trigger described in the original whitepaper because it can trigger the authentication attempt *without* any credentials. It should also be noted that because the AD CS endpoint is HTTP and the incoming authentication uses SMB, the protections provided by MS08-068 do not apply.

Testing Results

Rapid7 researchers who tested the PetitPotam attack chain in August 2021 observed the following behavior:

- Windows Domain Controllers with **and** without Active Directory Certificate Services running were exploitable **unauthenticated** out of the box.
- A non-DC system was exploitable **authenticated** out of the box, whether or not it was joined to the domain.
- The non-DC system was exploitable **unauthenticated** by adding the lsarpc named pipe to the server's allowlist for anonymous access. That configuration parameter can be found here. Note the differences in default values depending on the server designation.

Rapid7 Customers

InsightVM and Nexpose customers can assess their exposure to PetitPotam via the local vulnerability checks msft-adv210003, which looks for the registry settings described in ADV210003, and msft-cve-2021-36942, which checks for the patches released by Microsoft on August 10.

Updates

August 23, 2021: Multiple sources have now reported that at least one ransomware gang (LockFile) is chaining ProxyShell with PetitPotam (CVE-2021-36942) to compromise Windows domain controllers. See Rapid7's blog on ProxyShell for further information on mitigation and attack chain analysis.

August 10, 2021: Microsoft has released a patch that addresses the PetitPotam NTLM relay attack vector in today's Patch Tuesday. Tracked as CVE-2021-36942, the August 2021 Patch Tuesday security update blocks the affected API calls OpenEncryptedFileRawA and OpenEncryptedFileRawW through the LSARPC interface. Windows administrators should prioritize patching domain controllers and will still need to take additional steps listed in KB5005413 to ensure their systems are fully mitigated.
