



Software Engineering Institute

CERT Coordination Center

Home	Notes	Search	Report a Vulnerability	Disclosure Guidance	VINCE
----------------------	-----------------------	------------------------	--	-------------------------------------	-----------------------

[Home](#) > [Notes](#) > VU#405600

Microsoft Windows Active Directory Certificate Services can allow for AD compromise via PetitPotam NTLM relay attacks

Vulnerability Note VU#405600



Original Release Date: 2021-08-02 | Last Revised: 2021-10-05

Overview

Microsoft Windows Active Directory Certificate Services (AD CS) by default can be used as a target for NTLM relay attacks, which can allow a domain-joined computer to take over the entire Active Directory.

Description

[PetitPotam](#) is a tool to force Windows hosts to authenticate to other machines by using the [Encrypting File System Remote \(EFSRPC\)](#) [EfsRpcOpenFileRaw](#) and other methods. When a system handles certain EFSRPC requests, it will by default use NTLM to authenticate with the host that is specified within the path to the file specified in the EFSRPC request. The user specified in the NTLM authentication information is the computer account of the machine that made the EFSRPC request.

Code running on any domain-joined system will leverage Single Sign-On (SSO) to call these EFSRPC functions on a domain controller without needing to know the credentials of the current user or any other user in an Active Directory. And because the EFSRPC methods authenticate as the machine dispatching the request, this means that a user of any system connected to an AD domain can trigger an NTLM authentication request as the domain controller machine account to an arbitrary host, without needing to know any credentials. This can allow for NTLM relay attacks. Furthermore, the [EfsRpcOpenFileRaw](#) function can be invoked in a truly anonymous manner, without requiring credentials via SSO or other means.

One publicly-discussed target for an NTLM relay attack from a domain controller is a machine that hosts [Microsoft AD CS](#). By relaying an NTLM authentication request from a domain controller to the Certificate Authority Web Enrollment or the Certificate Enrollment Web Service on an AD CS system, an attacker can obtain a certificate that can be used to obtain a Ticket Granting Ticket (TGT) from the domain controller. This attack, known as a "Golden Ticket" attack, can be used to fully compromise the entire Active Directory infrastructure.

Although Microsoft refers to this entire attack chain as "PetitPotam" in [KB5005413](#), it is important to realize that PetitPotam is simply the single PoC exploit used to invoke an NTLM authentication request by way of a [EfsRpcOpenFileRaw](#) request. It should be noted that:

1. There may be other techniques that may cause a Windows system to initiate a connection to an arbitrary host using privileged NTLM credentials.
2. There may be services other than AD CS that may be leveraged to use as a target for a relayed NTLM authentication request.

Impact

By making a crafted RPC request to a vulnerable Windows system, a remote attacker may be able to leverage the NTLM authentication information that is included in the request that is generated. In the case of AD CS, this can allow an attacker on any domain-joined system to be able to compromise the Active Directory.

Solution

Apply an update

This issue is partially addressed in the [Microsoft update for CVE-2021-36942](#). This update blocks the unauthenticated [EfsRpcOpenFileRaw](#) API call that is exposed through the LSARPC interface. Note that the EFSRPC interface for accessing [EfsRpcOpenFileRaw](#) is still reachable to authenticated users after installing this update. In addition, other EFSRPC functions that require authentication to exploit are still exposed to users via LSARPC after this update is installed. This required authentication may take place silently via SSO on domain-joined systems. Please see [KB5005413](#) for several additional workarounds that can help mitigate other techniques for relaying NTLM credentials using an AD CS server.

Enable Extended Protection for Authentication (EPA) and Require SSL on AD CS systems

[ABOUT
VULNERABILITY
NOTES](#)

[CONTACT US ABOUT
THIS
VULNERABILITY](#)

[PROVIDE A VENDOR
STATEMENT](#)

Please see [KB5005413](#) for more details about enabling EPA to help protect against this weakness. It is important to note:

1. In addition to configuring EPA through the IIS Manager GUI, the Certificate Enrollment Web Service (CES) also requires modifying the `web.config` file to successfully enable EPA.
2. The CES and the CertSrv applications **must** be configured to enable the **Require SSL** option for EPA protection to work. If **Require SSL** is not enabled, then any changes to the EPA settings will not have any effect.

Disable incoming NTLM on AD CS servers

The stage of leveraging an AD CS server to achieve the ability to get a TGT can be mitigated by disabling incoming NTLM support on AD CS servers. To configure this GPO setting, go to: **Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options** and set **Network security: Restrict NTLM: Incoming NTLM traffic** to **Deny All Accounts** or **Deny All domain accounts**

Note that the group policy may need to be refreshed on the AD CS server for this mitigation to take effect.

Disable the NTLM provider in IIS

For both the "Certificate Authority Web Enrollment" (CES) service (`<CA_INFO>-CA_CES_Kerberos` in IIS Manager) and the "Certificate Enrollment Web Service" (`CertSrv` in IIS Manager) services:

1. Open IIS Manager
2. Select Sites -> Default Web Site (or another name if it was manually reconfigured) -> `*-`
`CA_CES_Kerberos` and `CertSrv`
3. Select `Windows Authentication`
4. Click the `Providers...` link on the right side
5. Select `NTLM`
6. Click the `Remove` Button
7. Restart IIS from an Administrator CMD prompt: `iisreset /restart`

Block [MS-ESFR] (EFSRPC) using RPC filters

RPC filters can be used to block the (remote) EFSRPC functionality that PetitPotam uses. This can be done by blocking the [RPC interface UUIDs for EFSRPC](#).

First create a file called `block_efsrv.txt` and place the following contents in it:

```
rpc
filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=c681d488-d850-11d0-8c52-00c04fd90f7e
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=df1941c5-fe89-4e79-bf10-463657acf44d
add filter
quit
```

Then import the filter using the following command from an elevated-privileged command prompt:

```
netsh -f block_efsrv.txt
```

Alternatively, the above text block can be pasted into an interactive `netsh` session if you wish to avoid the use of a file to import the rules from.

The current filters can be viewed by running the following command:

```
netsh rpc filter show filter
```

All RPC filters can be removed using the following command:

```
netsh rpc filter delete filter filterkey=
```

This will restore Windows to its default configuration of not having any RPC filters. If you have other RPC filters in place and wish to remove only the EFSRPC filters, you can specify the specific `filterKey` values that are reported by the `show filter` command listed above.

Disable NTLM Authentication on your Windows domain controller

Instructions for disabling NTLM authentication in your domain can be found in the article [Network security: Restrict NTLM: NTLM authentication in this domain](#).

Note that existing logins may need to be terminated for this mitigation to take effect. Also note that disabling NTLM has been reported by some to be disruptive to expected network functionality. For this reason, please consider the other workarounds in this vulnerability note.

Acknowledgements

The PetitPotam aspect of this attack chain was publicly disclosed by topotam. The AD CS aspect was publicly disclosed by harmj0y (Will Schroeder) and tifkin_ (Lee Christensen).

This document was written by Will Dormann.

Vendor Information

Filter by status:

All

Filter by content:

☐ Additional information available

Sort by:

Status

[Expand all](#)

References

- <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942>
- <https://msrc.microsoft.com/update-guide/vulnerability/ADV210003>
- <https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>
- https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr
- https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr/ccc4fb75-1c86-41d7-bbc4-b278ec13bfb8
- <https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority>
- <https://msrc-blog.microsoft.com/2009/12/08/extended-protection-for-authentication/>
- <https://github.com/topotam/PetitPotam>
- <https://posts.specterops.io/certified-pre-owned-d95910965cd2>
- <https://www.exandroid.dev/2021/06/23/ad-cs-relay-attack-practical-guide/>

Other Information

CVE IDs: [CVE-2021-36942](#)

Date Public: 2021-08-02

Date First Published: 2021-08-02

Date Last Updated: 2021-10-05 12:12 UTC

Document Revision: 14

Sponsored by [CISA](#)

 [Download PGP Key](#)

[Read CERT/CC Blog](#)

[Learn about Vulnerability Analysis](#)


Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
[412-268-5800](tel:412-268-5800)

[Office Locations](#) | [Additional Sites Directory](#) | [Legal](#) | [Privacy Notice](#) | [CMU Ethics Hotline](#) | www.sei.cmu.edu

©2022 Carnegie Mellon University

[Contact SEI](#)

Contact CERT/CC

 [412-268-5800](tel:412-268-5800)

 cert@cert.org