CERT-EU

Security Advisory 2022-044

MS-DFSNM NTLM Relay Attack for Windows Domain Takeover

June 21, 2022 — v1.0

TLP:WHITE

History:

- *21/06/2022 — v1.0 – Initial publication*

Summary

On the 18th of June 2022, a security researcher published a proof of concept for MS-DFSNM coerce authentication using `NetrDfsRemoveStdRoot` method [1]. This type of attack allows Windows domain takeover. To coerce a remote server to authenticate against a malicious NTLM relay, threat actors could use various methods, including the MS-RPRN, MS-EFSRPC (PetitPotam), and MS-FSRVP protocols [2-7].

Technical Details

A Windows NTLM relay attack has been discovered that uses MS-DFSNM, Microsoft's Distributed File System [8], which can take over a Windows domain.

This service is vulnerable to NTLM relay attacks, which is when threat actors force, or coerce, a domain controller to authenticate against a malicious NTLM relay under an attacker's control.

This malicious server would then relay, or forward, the authentication request to a domain's Active Directory Certificate Services via HTTP and ultimately be granted a Kerberos ticket-granting ticket (TGT). This ticket allows the threat actors to assume the identity of any device on the network, including a domain controller.

Once they have impersonated a domain controller, they will have elevated privileges allowing the attacker to take over the domain and run any command. [2]

Recommendations

There are several mitigations against the aforementioned attack which are in general best practice and listed below [2].

- Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS) [9].
- Extended Protection for Authentication Overview [10] combined with signing featues, such as SMB signing, to protect Windows credentials [11].
- Use of Windows' built-in RPC Filters [12] or RPC Firewall [13] to prevent servers from being coerced via the MS-DFSNM protocol.

References

[1] https://github.com/Wh04m1001/DFSCoerce

[2] https://www.bleepingcomputer.com/news/microsoft/new-dfscoerce-ntlm-relay-attack-allows-windows-domain-takeover/

[3] http://www.thehacker.recipes/active-directory-domain-services/movement/mitm-and-coerced-authentications/ms-rprn

[4] https://www.bleepingcomputer.com/news/microsoft/new-petitpotam-attack-allows-take-over-of-windows-domains/

[5] https://github.com/ShutdownRepo/ShadowCoerce

[6] https://github.com/leechristensen/SpoolSample

[7] https://github.com/topotam/PetitPotam

[8] https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-dfsnm/95a506a8-cae6-4c42-b19d-9c1ed1223979

[9] https://support.microsoft.com/en-us/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

[10] https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/extended-protection-for-authentication-overview

[11] https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing

[12] https://www.akamai.com/blog/security/guide-rpc-filter#why

[13] https://zeronetworks.com/blog/the-ransomware-kill-switch-becomes-even-more-deadly-the-rpc-firewall-2-0-released/