AL2022_41 New DFSCoerce NTLM Relay attack allows Windows domain takeover (22nd June 2022)

Description

DFSCoerce is a new type of Windows NTLM (Windows New Technology LAN Manager) relay attack that uses the Distributed File System (DFS): Namespace Management Protocol (MS-DFSNM -Microsoft's Distributed File System) to completely take over a Windows domain.

Summary

Filip Dragovic, a security researcher, published the attack as a Proof-of-Concept (PoC) script. The script is based on the "DFSCoerce" NTLM relay attack, which relays authentication attempts against servers via Microsoft's Distributed File System. NTLM relay attacks basically allow an attacker to sit between clients and servers and relay validated authentication requests to gain access to network services.

How it Works

Microsoft Active Directory Certificate Services, a public key infrastructure (PKI) service used to authenticate users, services, and devices on a Windows domain. This service, however, is vulnerable to NTLM relay attacks, which occur when threat actors force or coerce a domain controller to authenticate against a malicious NTLM relay controlled by the attacker. The malicious server could then use HTTP to relay or forward the authentication request to a domain's Active Directory Certificate Services, where it would be granted a Kerberos ticket-granting ticket (TGT). This ticket enables threat actors to assume the identity of any network device, including a domain controller.
They will have elevated privileges once they have impersonated a domain controller, allowing the attacker to take over the domain and run any command. Threat actors could use a variety of methods, including the MS-RPRN, MS-EFSRPC (PetitPotam), and MS-FSRVP protocols, to force a remote server to authenticate against a malicious NTLM relay.

Remediation

Microsoft recommends enabling protections such as Extended Protection for Authentication (EPA), SMB signing, and turning off HTTP on AD CS servers to mitigate NTLM relay attacks.

The Guyana National CIRT recommends that users and administrators review these recommendations and implement them where necessary.

References

- Abrams, L. (2022, June 21). *New DFSCoerce NTLM Relay attack allows Windows domain takeover*. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/microsoft/new-dfscoerce-ntlm-relay-attack-allows-windows-domain-takeover/

- Lakshmanan, R. (2022, June 21). *New NTLM Relay Attack Lets Attackers Take Control Over Windows Domain*. Retrieved from The Hacker News. https://thehackernews.com/2022/06/new-ntlm-relay-attack-lets-attackers.html

- Paganini, P. (2022, June 21). *DFSCoerce NTLM relay attack allows taking control over Win domains*. Retrieved from Security Affairs. https://securityaffairs.co/wordpress/132473/hacking/dfscoerce-attacks-windows-domains.html