What is noPac (sAMAccountName spoofing)?

noPac (CVE-2021-42278 combined with CVE-2021-42287) is a privilege escalation from any authenticated user to Domain Admin. The attacker creates a machine account, renames its sAMAccountName to match a domain controller (dropping the trailing dollar sign), requests a TGT, renames it back, and then uses S4U2self to get a service ticket as a privileged user, because a KDC validation flaw resolves the ticket to the DC. Defend by patching and setting the machine account quota to zero.

HOW IT WORKS

01 How the attack works

By default any authenticated user can create machine accounts (ms-DS-MachineAccountQuota is 10). The attacker creates one, renames its sAMAccountName to a DC's name without t he trailing dollar sign, requests a TGT, r enames the account back, then requests an S 4U2self ticket for a privileged user, which t he KDC issues as the DC. Tools such as `noPac.py -dc-ip <dc> <domain>/<user>:<pass> --impersonate administrator -dump` automate the whole chain. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: CVE-2021-42278 SAM name spoofing

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/nopac-samaccountname-spoofing

Open online