What is Zerologon?

Zerologon (CVE-2020-1472) is a critical flaw in the Netlogon Remote Protocol's use of AES-CFB8: a fixed i nitialization vector made one in 256 all-zero challenges validate, so an unauthenticated attacker on t he network could impersonate a domain controller and reset the DC's machine account password to em pty in seconds. From there they perform DCSync and dump every hash, full domain compromise wi th no credentials. It is fully patched; the fix (August 2020) enforces secure Netlogon. Defend by pa tching and enforcing secure RPC.

HOW IT WORKS

01 How the attack works

The attacker repeatedly sends Netlogon authentication with zeroed values until one validates (a few seconds), then calls NetrServerPasswordSet2 to set the DC's machine a ccount password to empty. With that t hey authenticate as the DC and run D CSync (`secretsdump.py`) to dump the KRBTGT and all account hashes. Note that resetting the DC password can break the DC if not restored, so the technique carries real operational risk. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: CVE-2020-1472 Netlogon Elevation of Privilege

Test your Active Directory before an attacker does.

`securelayer7.net/learn/active-directory/zerologon`

Open online