What is ESC4?

ESC4 is an AD CS abuse where an attacker holds write permissions over a certificate template (for example GenericWrite, WriteDACL, or WriteOwner). Instead of finding a misconfigured template, they make one: edit a safe template to become ESC1-vulnerable, request a certificate as a Domain Admin, then revert the template to hide the change. It links ACL abuse and AD CS into one escalation, and Certipy can perform the whole sequence.

HOW IT WORKS

01 The abuse and payload

Certipy can weaponise the write access, exploit, and roll back:

- Make the template vulnerable (and save the original): `certipy template -u user@corp.local -p pass -template VulnTemplate -save-old`
- Run the ESC1 flow: `certipy req -u user@corp.local -p pass -ca CORP-CA -template VulnTemplate -upn administrator@corp.local`
- Authenticate, then restore the template to its prior state.

The revert is what makes ESC4 quiet. Shown here for defensive awareness.

> WHY IT HIDES
>
> *ESC4 leaves the template looking normal afterward, because the attacker reverts it. The detectable moment is the write to the template object, not the template state.*

HOW TO DEFEND

- Audit template permissions. No low-privileged principal should have GenericWrite, WriteDACL, WriteOwner, or GenericAll over a certificate template.
- Tighten template ACLs to the minimum administrative set.
- Monitor for changes to template objects, since the modification is the real attack signal.
- Run BloodHound and Certipy together to find who can write which templates.

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-esc4

Open online