What is ESC1?

ESC1 is a certificate-template misconfiguration in Active Directory Certificate Services (AD CS), one of the publicly documented ESC abuse classes. It exists when a template allows low-privileged users to enrol, permits client authentication, and lets the requester supply the subject (the identity) in the request. Put together, those three settings let an ordinary user request a certificate that says they are a Domain Admin, then use it to authenticate as that admin. It is one of the fastest paths from a normal account to full domain control, and tools like Certipy find and exploit it in seconds.

HOW IT WORKS

01 The escalation it gives away

A certificate that proves identity is, in effect, a credential. With ESC1, a low-privileged user requests a certificate and sets the subject to a privileged account, for example `administrator@corp.local`.

The certificate authority issues it. The attacker then uses that certificate to obtain a Kerberos TGT as the Domain Admin and acts with full privileges. No password, no hash cracking, just a certificate the environment was configured to hand out. Because certificates stay valid for a long time, the same certificate also works as quiet persistence that survives password resets.

02 How the attack runs

Certipy automates the whole chain. The published steps are:

- Find vulnerable templates: `certipy find -u user@corp.local -p pass -dc-ip <ip> -vulnerable`
- Request a certificate impersonating an admin: `certipy req -u user@corp.local -p pass -ca CORP-CA -template VulnTemplate -upn administrator@corp.local`
- Authenticate with the issued certificate to get the admin's hash or a TGT: `certipy auth -pfx administrator.pfx -dc-ip <ip>`

Three commands take a standard user to Domain Admin. These are documented techniques shown so defenders can recognise and close the path.

HOW TO DEFEND

- Audit every template with Certipy or PSPKIAudit and flag any that lets the enrollee supply the subject while allowing low-privileged enrolment and client authentication.
- Turn off "supply subject in request" on authentication templates, or require manager approval so a human signs off on each issuance.
- Tighten enrolment permissions so broad groups like Domain Users cannot enrol in sensitive templates.
- Monitor certificate issuance and treat any request that names a privileged identity as a high-severity alert.
- Reissue after suspected abuse, because a malicious certificate survives password resets.

SOURCES

[1] Microsoft: Active Directory Certificate Services

[2] MITRE ATT&CK Enterprise Matrix

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

THE SETTING THAT CAUSES IT

The single most important flag is "supply subject in request" (ENROLLEE_SUPPLIES_SUBJECT) on a template that low-privileged users can enrol in and that allows authentication. Remove that combination and ESC1 disappears.

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/what-is-esc1

Open online