What is ESC7?

ESC7 is an AD CS abuse where a low-privileged account holds CA management rights: Manage CA (ManageCA) or Manage Certificates (ManageCertificates). With these, an attacker can enable the dangerous ESC6 SAN flag, approve their own pending certificate requests, or otherwise bend the CA to issue a privileged certificate. CA roles are powerful and often over-granted, which is why auditing who holds them is essential. Certipy can drive the abuse.

HOW IT WORKS

01 The abuse and payload

Certipy can leverage CA rights directly. Common chains:

- With Manage CA, enable the SAN flag (then exploit as ESC6): `certipy ca -u user@corp.local -p pass -ca CORP-CA -enable-template ... /set` the EditFlags
- Add an officer / approve own request with Manage Certificates: `certipy ca -ca CORP-CA -issue-request <id>`
- Then request a privileged certificate and authenticate.

The exact commands depend on which right is held. Shown for defensive awareness.

> CA ROLES ARE TIER 0
>
> *Manage CA and Manage Certificates are as powerful as Domain Admin in practice, because they control who the domain will vouch for. Grant them like you grant DA.*

HOW TO DEFEND

- Audit who holds Manage CA and Manage Certificates. They should belong to a small, trusted administrative set only.
- Remove these rights from low-privileged or service accounts.
- Require separation of duties so the same person cannot both submit and approve sensitive requests.
- Monitor CA configuration changes (especially the SAN flag) and certificate approvals.
- Enumerate with Certipy, which reports CA role holders.

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-esc7

Open online