What is ESC2?

ESC2 is an AD CS template misconfiguration where a low-privileged user can enrol in a template that defines "Any Purpose" (or no) Extended Key Usage. The issued certificate is not limited to one use, so it can be repurposed for client authentication to log in as the requester, or used in further abuse. Like ESC1 it turns a careless template into a path toward privilege, and Certipy finds and exploits it.

HOW IT WORKS

01 The abuse and payload

An attacker enumerates templates, finds the any-purpose one they can enrol in, requests a certificate, and uses it to authenticate or to sign further certificates.

- Find it: `certipy find -u user@corp.local -p pass -dc-ip <ip> -vulnerable`
- Request the certificate: `certipy req -u user@corp.local -p pass -ca CORP-CA -template AnyPurposeTemplate`
- Authenticate with it: `certipy auth -pfx user.pfx -dc-ip <ip>`

These are documented Certipy steps shown so defenders recognise the pattern.

> **ESC1 VS ESC2**
>
> *ESC1 = the requester names the subject (who the cert is for). ESC2 = the certificate has no usage limit (Any Purpose EKU). Both start from a template a low-privileged user can enrol in.*

HOW TO DEFEND

- Audit templates for the Any Purpose EKU (or empty EKU) combined with low-privileged enrolment. Certipy and PSPKIAudit flag them.
- Set a specific, minimal EKU on every authentication template instead of Any Purpose.
- Require manager approval on sensitive templates.
- Restrict enrolment so broad groups cannot request these certificates.
- Monitor issuance of any-purpose certificates as a high-severity event.

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-esc2

Open online