AD CS attacks (ESC1 to ESC8).

Active Directory Certificate Services (AD CS) is the in-house certificate authority many Windows networks run to issue certificates for logon, VPN, and more. Security researchers have publicly documented a family of misconfigurations, numbered ESC1 to ESC8, where a low-privileged user can request or forge a certificate that authenticates them as a privileged account. Because a certificate can be used to get a Kerberos ticket, a single bad template setting can take an attacker from ordinary user to Domain Admin in minutes, often quietly. Tools like Certipy automate finding and abusing these paths.

HOW IT WORKS

01 The ESC family, in plain terms

Security researchers documented the misconfiguration classes ESC1 to ESC8. A few of the common ones:

- ESC1: a certificate template lets a low-privileged user request a certificate and specify any identity (subject), so they ask for one as a Domain Admin and get it.
- ESC2 / ESC3: overly permissive templates or agent certificates that can be repurposed to enrol on behalf of others.
- ESC4: the attacker has write access to a template and edits it to become vulnerable, then exploits it.
- ESC6: a CA-wide flag that lets requesters specify the subject regardless of template.
- ESC8: an NTLM relay to the certificate authority's web enrolment endpoint, often combined with coercing a Domain Controller to authenticate, yielding a DC certificate.

The details differ, but the outcome is the same: a certificate that authenticates as someone privileged.

02 Why it is so dangerous

AD CS abuse is favoured for three reasons:

- It often needs only a low-privileged user to reach Domain Admin in one or two steps.

HOW TO DEFEND

- Audit every certificate template for the ESC conditions, especially templates that allow the requester to supply the subject and that permit low-privileged enrolment. Certipy and PSPKIAudit can find them.
- Remove the "supply subject in request" right where it is not strictly needed, and tighten enrolment permissions.
- Disable NTLM on the CA web enrolment endpoints and enforce signing to kill ESC8 relay.
- Monitor certificate issuance and treat a certificate request that names a privileged identity as a high-severity alert.
- Revoke and reissue if abuse is suspected, since a forged certificate is not cleared by a password reset.

SOURCES

[1] Microsoft: Active Directory Certificate Services

[2] MITRE ATT&CK Enterprise Matrix

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

- Certificates are long-lived. A stolen or forged certificate can remain valid for a year or more, surviving the password resets that would otherwise evict an attacker. This makes it a stealthy persistence mechanism, not just an escalation.
- It is under-monitored. Many teams do not watch certificate enrolment the way they watch logons, so the abuse is quiet.

Test your Active Directory before an attacker does.
securelayer7.net/learn/active-directory/ad-cs-esc-attacks

Open online