Identify insecure AD CS certificate enrollment IIS endpoints (ESC8) - Microsoft Defender for Identity

learn.microsoft.com/en-us/defender-for-identity/security-assessment-insecure-adcs-certificate-enrollment

AbbyMSFT

This article describes Microsoft Defender for Identity's **Edit insecure ADCS certificate enrollment IIS endpoints** identity security posture assessment report.

Active Directory Certificate Services (AD CS) supports certificate enrollment through various methods and protocols, including enrollment via HTTP using the Certificate Enrollment Service (CES) or the Web Enrollment interface (Certsrv).

If the IIS endpoint allows NTLM authentication without enforcing protocol signing (HTTPS) or without enforcing Extended Protection for Authentication (EPA), it becomes vulnerable to NTLM relay attacks (ESC8). Relay attacks can lead to complete domain takeover if an attacker manages to pull it off successfully.

This assessment is available only to customers who have installed a sensor on an AD CS server. For more information, see Configuring sensors for AD FS and AD CS.

Review the recommended action at https://security.microsoft.com/securescore?viewid=actions for insecure AD CS certificate enrollment IIS endpoints.

The assessment lists the problematic HTTP endpoints in your organization and guidance to configuring the endpoints securely.

Once handled, the ESC8 attack risk is mitigated, reducing your attack surface significantly.

Note

While assessments are updated in near real time, scores and statuses are updated every 24 hours. While the list of impacted entities is updated within a few minutes of your implementing the recommendations, the status may still take time until it's marked as **Completed**.

- Learn more about Microsoft Secure Score
- Check out the Defender for Identity forum!