Edit misconfigured Certificate Authority ACL (ESC7) - Microsoft Defender for Identity

learn.microsoft.com/en-us/defender-for-identity/security-assessment-edit-misconfigured-ca-acl

AbbyMSFT

Screenshot of the Edit misconfigured Certificate Authority ACL (ESC7) recommendation.

11/27/2024

This article describes Microsoft Defender for Identity's **Misconfigured certificate authority ACL** security posture assessment report.

Certificate Authorities (CAs) maintain access control lists (ACLs) that outline roles and permissions for the CA. If access control isn't configured correctly, any user might be allowed to interfere with the CA settings, circumventing security measures, and potentially compromise the entire domain.

The effect of a misconfigured ACL varies based on the type of permission applied. For example:

- If an unprivileged user holds the *Manage Certificates* right, they can approve pending certificate requests, bypassing the *Manager approval* requirement.

- With the *Manage CA* right, the user can modify CA settings, such as adding the *User specifies SAN* flag (`EDITF_ATTRIBUTESUBJECTALTNAME2`), creating an artificial misconfiguration that might later lead to a complete domain compromise.

This assessment is available only to customers who installed a sensor on an AD CS server. For more information, see New sensor type for Active Directory Certificate Services (AD CS).

1. Review the recommended action at https://security.microsoft.com/securescore?viewid=actions for misconfigured Certificate Authority ACLs. For example:

   Screenshot of the Edit misconfigured Certificate Authority ACL (ESC7) recommendation.

2. Research why the CA ACL is misconfigured.

3. Remediate the issues by removing all permissions that grant unprivileged built-in groups with *Manage CA* and/or *Manage certificates* permissions.

Make sure to test your settings in a controlled environment before turning them on in production.

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!

Training

Module

Manage security in Active Directory - Training

This module focuses on maintaining security in an Active Directory environment. It covers things from permissions management to authentication methods to identifying problematic accounts.

Certification

Microsoft Certified: Information Security Administrator Associate - Certifications

As an Information Security Administrator, you plan and implement information security of sensitive data by using Microsoft Purview and related services.