Edit vulnerable Certificate Authority setting (ESC6) - Microsoft Defender for Identity

learn.microsoft.com/en-us/defender-for-identity/security-assessment-edit-vulnerable-ca-setting

AbbyMSFT

11/27/2024

This article describes Microsoft Defender for Identity's **Vulnerable Certificate Authority setting** report.

Each certificate is associated with an entity through its subject field. However, a certificate also includes a *Subject Alternative Name* (SAN) field, which allows the certificate to be valid for multiple entities.

The SAN field is commonly used for web services hosted on the same server, supporting the use of a single HTTPS certificate instead of separate certificates for each service. When the specific certificate is also valid for authentication, by containing an appropriate EKU, such as *Client Authentication*, it can be used to authenticate several different accounts.

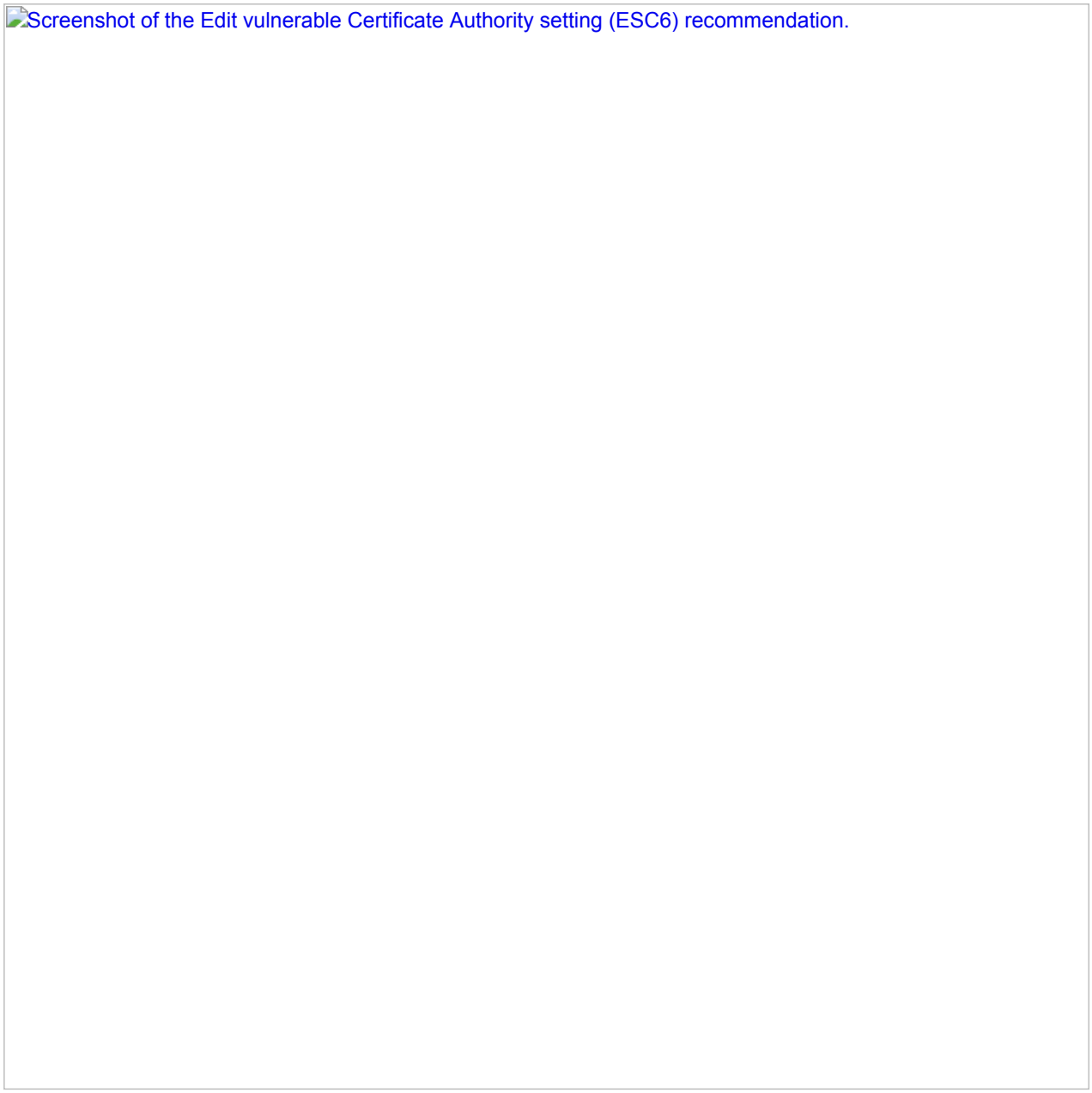
Unprivileged users that can specify the users in the SAN settings can lead to immediate compromise, and post a great risk to your organization.

If the AD CS `editflags` > `EDITF_ATTRIBUTESUBJECTALTNAME2` flag is turned on, each user can specify the SAN settings for their certificate request. This, in turn affects all certificate templates, whether they have the `Supply in the request` option turned on or not.

If there's a template where the `EDITF_ATTRIBUTESUBJECTALTNAME2` setting is turned on, and the template is valid for authentication, an attacker can enroll a certificate that can impersonate any arbitrary account.

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 editing vulnerable Certificate Authority settings. For example:

2. Research why the `EDITF_ATTRIBUTESUBJECTALTNAME2` setting is turned on.

3. Turn off the setting by running:

   Windows Command Prompt

   ```
   certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2
   ```

4. Restart the service by running:

   Windows Command Prompt

   ```
   net stop certsvc & net start certsvc
   ```

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

Implement and manage Active Directory Certificate Services - Training

Implement and manage Active Directory Certificate Services

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.