Prevent users to request a certificate valid for arbitrary users based on the certificate template (ESC1) - Microsoft Defender for Identity

learn.microsoft.com/en-us/defender-for-identity/security-assessment-prevent-users-request-certificate

AbbyMSFT

Screenshot of the Prevent users to request a certificate valid for arbitrary users based on the certificate template (ESC1) recommendation.

11/27/2024

This article provides describes Microsoft Defender for Identity's **Prevent users to request a certificate valid for arbitrary users based on the certificate template (ESC1)** identity security posture assessment report.

Each certificate is associated with an entity through its subject field. However, certificates also include 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.

If a certificate template has the *Supply in the request* option turned on, the template is vulnerable, and attackers might be able to enroll a certificate that's valid for arbitrary users.

Important

If the certificate is also permitted for authentication and there aren't any mitigation measures enforced, such as *Manager approval* or required authorized signatures, the certificate template is dangerous as it allows any unprivileged user to take over any arbitrary user, including a domain admin user.

This specific setting is one of the most common misconfigurations.

1. Review the recommended action at https://security.microsoft.com/securescore?viewid=actions for certificate requests for arbitrary users. For example:

   Screenshot of the Prevent users to request a certificate valid for arbitrary users based on the certificate template (ESC1) recommendation.

2. To remediate certificate requests for arbitrary users, perform at least one of the following steps:
    - Turn off *Supply in the request* configuration.
    - Remove any EKUs that enable user authentication, such as *Client Authentication*, *Smartcard logon*, *PKINIT client authentication*, or *Any purpose*.
    - Remove overly permissive enrollment permissions, which allow any user to enroll certificate based on that certificate template.

      Certificate templates marked as vulnerable by Defender for Identity have at least one access list entry that supports enrollment for a built-in, unprivileged group, making this exploitable by any user. Examples of built-in, unprivileged groups include *Authenticated Users* or *Everyone*.
    - Turn on the CA certificate *Manager approval* requirement.
    - Remove the certificate template from being published by any CA. Templates that aren't published can't be requested, and therefore can't be exploited.

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

Secure Windows Server user accounts - Training

Protect your Active Directory environment by securing user accounts to least privilege and placing them in the Protected Users group. Learn how to limit authentication scope and remediate potentially insecure 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.