Edit overly permissive certificate template with privileged EKU (Any purpose EKU or No EKU) (ESC2) - Microsoft Defender for Identity

learn.microsoft.com/en-us/defender-for-identity/security-assessment-edit-overly-permissive-template

AbbyMSFT

11/27/2024

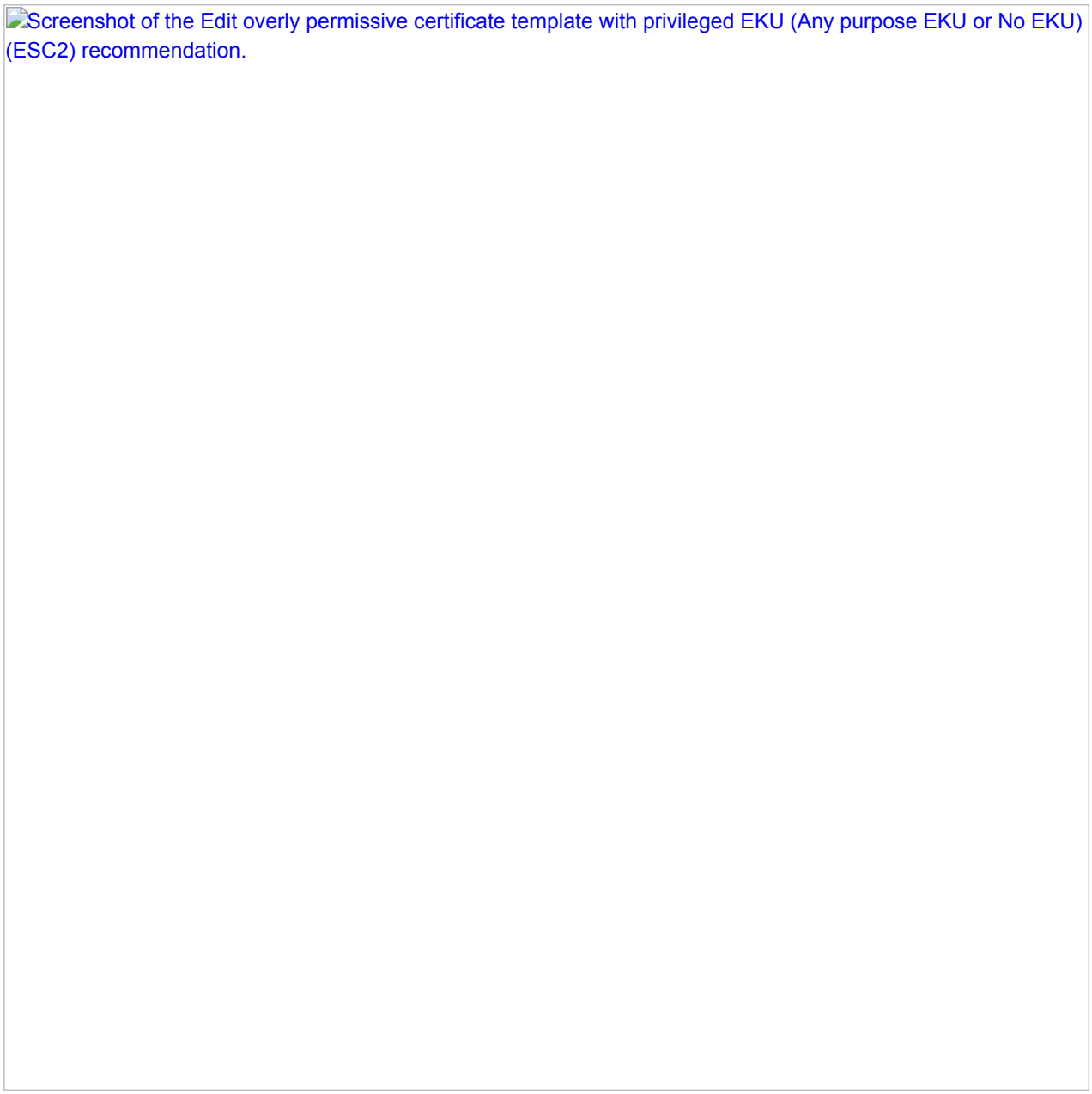
This article describes Microsoft Defender for Identity's **Overly permissive certificate template with privileged EKU** security posture assessment report.

Digital certificates play a vital role in establishing trust and preserving integrity throughout an organization. This is true not only in Kerberos domain authentication, but also in other areas, such as code integrity, server integrity, and technologies that rely on certificates like Active Directory Federation Services (AD FS) and IPSec.

When a certificate template has no EKUs or has an *Any Purpose* EKU, and it's enrollable for any unprivileged user, certificates issued based on that template can be used maliciously by an adversary, compromising trust.

Even though the certificate can’t be used for impersonating user authentication, it compromises other components that relieve digital certificates for their trust model. Adversaries can craft TLS certificates and impersonate any website.

1. Review the recommended action at https://security.microsoft.com/securescore?viewid=actions for overly permissive certificate templates with a privileged EKU. For example:

2. Research why the templates have a privileged EKU.

3. Remediate the issue by doing the following:

   - Restrict the template's overly permissive permissions.
   - Enforce extra mitigations like adding *Manager approval* and signing requirements if possible.

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

Design Solutions for Securing Privileged Access - Training

You learn advanced techniques for designing solutions that manage privileged access effectively.

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.