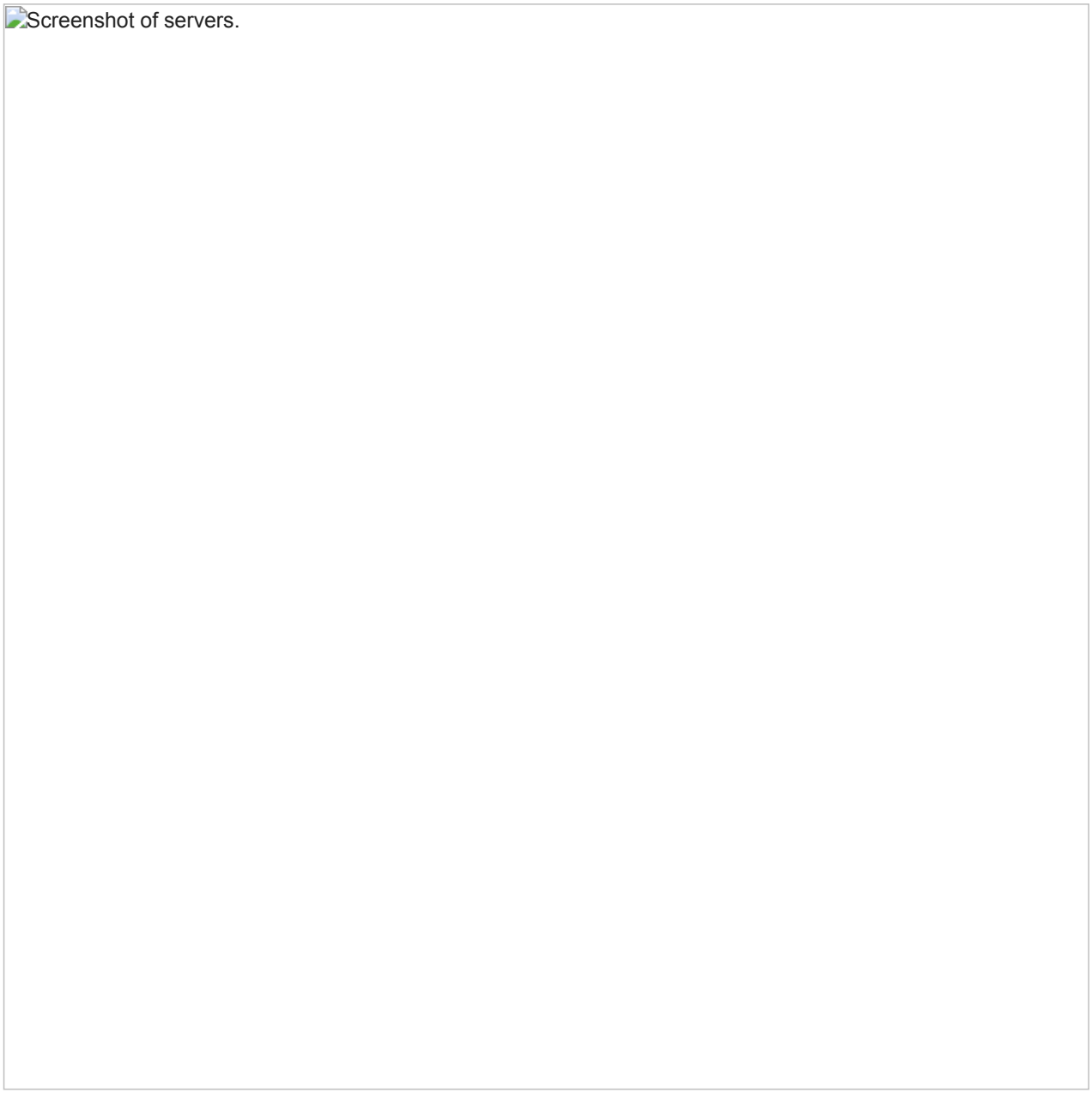
Security assessment: Prevent Certificate Enrollment with arbitrary Application Policies (ESC15)

learn.microsoft.com/en-us/defender-for-identity/prevent-certificate-enrollment-esc15

LiorShapiraa



12/06/2024

This article describes Microsoft Defender for Identity's Prevent Certificate Enrollment with arbitrary Application Policies (ESC15) security posture assessment report.

This recommendation directly addresses the recently published CVE-2024-49019, which highlights security risks associated with vulnerable AD CS configurations. This security posture assessment lists all vulnerable certificate templates found in customer environments due to unpatched AD CS servers.

Certificate templates that are vulnerable to CVE-2024-49019 allow an attacker to issue a certificate with arbitrary Application Policies and Subject Alternative Name. The certificate can be used to escalate privileges, possibly resulting with full domain compromise.

These certificate templates expose organizations to significant risks, as they enable attackers to issue certificates with arbitrary Application Policies and Subject Alternative Names (SANs). Such certificates can be exploited to escalate privileges and potentially compromise the entire domain. In particular, these vulnerabilities allow non-privileged users to issue certificates that can authenticate as high-privileged accounts, posing a severe security threat.

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 Prevent Certificate Enrollment with arbitrary Application Policies (ESC15).
2. **Identify the vulnerable certificate templates:**
    - Remove enrollment permission for unprivileged users.
    - Disable the **"Supply in the request"** option.
3. Identify the AD CS servers which are vulnerable to CVE-2024-49019 and apply the relevant patch.

    For example:

- 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.