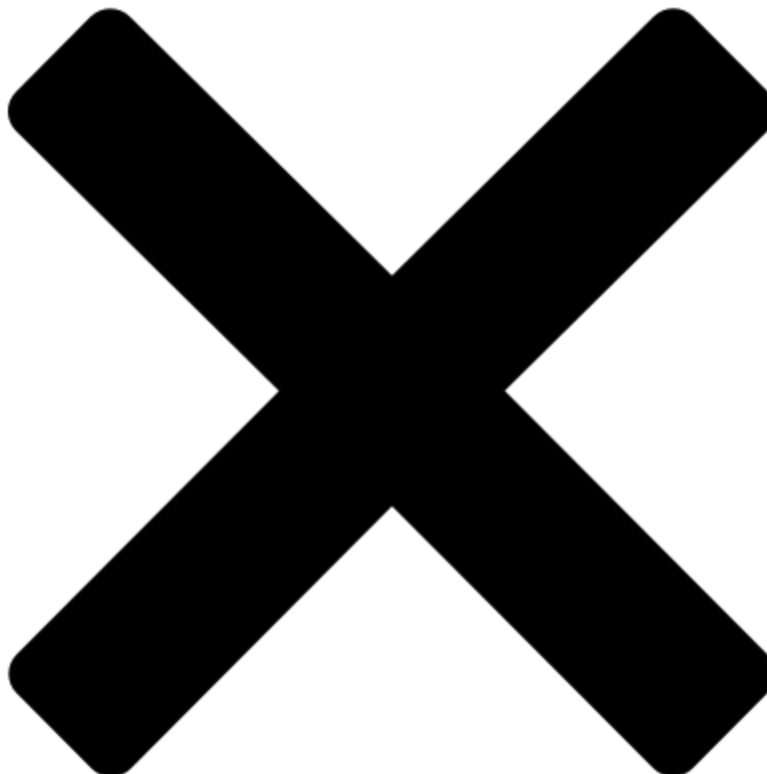


Defend Against the Latest Active Directory Certificate Services Threats

 [mandiant.com/blog/resources/defend-ad-cs-threats](https://www.mandiant.com/blog/resources/defend-ad-cs-threats)



Breadcrumb

1. [Home](#)
2. Defend Against the Latest Active Directory Certificate Services Threats

Blog

Matthew McWhirt, Thirumalai Natarajan, Phil Pearce, Jennifer Guzzetta

Jul 10, 2023

2 min read

| Last updated: Aug 01, 2023

prevention

Detection

Response

Active Directory Certificate Services (AD CS) is a server role that enables organizations to leverage public key infrastructure (PKI) as part of their on-premises services to issue and use digital certificates for authenticating identities and endpoints in Active Directory environments. As highlighted by SpecterOps in 2021, [AD CS has become a prime target and leverage point in the overall attack chain to achieve post-compromise objectives.](#)

AD CS is often challenging for cyber defenders to manage because not only is it difficult for security teams to detect when their AD CS has been compromised or leveraged for persistence, but the actual remediation and hardening steps can be rather complex.

To add to that complexity, while Microsoft has released updates to mitigate specific AD CS abuse scenarios, the updates are not cookie-cutter, and require organizations to thoroughly test and validate their configurations [prior to February 2025](#). After this date, AD CS will transition to a mode that could potentially impact domain-based services, specifically when certificates are utilized to authenticate users or endpoints.

To help security professionals understand the complexities of AD CS and how to mitigate its abuse, Mandiant has published a [hardening guide](#) that focuses on the most impactful AD CS attack techniques and abuse scenarios we are seeing on the frontlines of the latest breaches and attacks.

Additionally, this guide outlines actionable steps you can immediately take to identify misconfigurations and gaps in your AD CS environment that may result in compromise or attacker persistence, including:

1. Detailed mitigation and hardening instructions to minimize the impact of identified abuse techniques
2. Best practices to enhance visibility of your infrastructure that leverages AD CS
3. Hunting scenarios and PowerShell queries used to realize potential evidence of AD CS exploitation or misconfigured settings
4. Clarity regarding patches introduced by Microsoft for certificate-based authentication

To get started, read [Mandiant's Active Directory Certificate Services: Modern Attack Paths, Mitigations, and Hardening Guide](#) now.

To learn more about how Mandiant can help improve your Active Directory security posture, view our related resources:

1. [M-Trends 2022 Active Directory Misconfigurations: Webinar Playback](#) — Hear from Mandiant experts about specific Active Directory (AD) configuration missteps that put organizations at a higher risk for harmful compromise—in turn calling for increased focus on AD hardening setup and processes.
2. [Mandiant Active Directory Security Assessment: Datasheet](#) — Learn how Mandiant can help evaluate your existing architecture (on-premise and cloud environments) and identify potential high-risk attack paths within your Active Directory infrastructure.

THE
DEFENDER'S
[ADVANTAGE]

A GUIDE TO ACTIVATING CYBER DEFENSE

Cyber Defense Self-Assessment

Determine your cyber defense effectiveness

Validated by ESG

[Take The Assessment](#)

Have questions? Let's talk.

Mandiant experts are ready to answer your questions.

[Contact Us](#)