

No Exploit Required:

Why AD CS Keeps Getting You Domain Admin

Zach Tackett

Security Consultant

secureideas.com



professionally evil®

Who Am I?

Zach Tackett

Security Consultant

- Joined Secure Ideas Sep, 2025
- Penetration Testing
  - Internal/External networks
  - Web, Mobile applications & API's
- Background - Software Development and Cybersecurity Engineering
- Previous - Cybersecurity Engineer @ Booz Allen supporting NASA

PJPT, CySA+, Msc. Cybersecurity

- Marshall University Alum

Copyright © 2026 Secure Ideas LLC

“Wait...

You can get Domain Admin *THAT* easily?”

My first experience watching an AD CS attack



Copyright © 2026 Secure Ideas LLC

Nerd Time

Copyright © 2026 Secure Ideas LLC

So I Built a Lab…

Because apparently watching one AD CS attack wasn't enough.

GOAD — Game of Active Directory

- Isolated, intentionally vulnerable AD environment
- Hands-on testing of AD CS and other attack paths
- Paths to Power in Active Directory — Secure Ideas blog series

Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

Working as Configured, Still Vulnerable

If it ain't broke, don't fix it *- Made famous by Thomas "Bert" Lance, Director of the OMB under Carter*

- Software vulnerability not required
- Functioning as intended
- Lack of least privilege
- Lack of ongoing security reviews

Copyright © 2026 Secure Ideas LLC

Examples…

Enrollment for Domain Users or Domain Computers

Supply in the request

No Manager approval

0 authorized signatures required

Convenience Over Security

- Reusing templates for multiple purposes
- Relaxing approval requirements
- Keeping legacy enrollment services enabled

Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

```
Certificate Authorities                : ESSOS-CA
Enabled                                : True
Client Authentication                  : True
Enrollment Agent                       : False
Any Purpose                            : False
Enrollee Supplies Subject              : True
Certificate Name Flag                  : EnrolleeSuppliesSubject
Extended Key Usage                     : Client Authentication
Requires Manager Approval              : False
Requires Key Archival                  : False
Authorized Signatures Required         : 0
Schema Version                         : 2
Validity Period                        : 1 year
Renewal Period                         : 6 weeks
Minimum RSA Key Length                 : 2048
Template Created                       : 2025-12-16T22:00:03+00:00
Template Last Modified                 : 2025-12-16T22:00:04+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights                  : ESSOS.LOCAL\Domain Users
```

Least Privilege Doesn't Stop at User Accounts

- Broad enrollment permissions
- Unnecessary authentication capabilities
- Requester supplied info
- Permissions not audited

Copyright © 2026 Secure Ideas LLC

The Problem With Default Configurations

- Default settings aren't always appropriate
- Duplicated templates
- Carry over from older deployments
- Security settings rarely revisited

Copyright © 2026 Secure Ideas LLC



Who's Watching the Templates?

- Templates created and forgotten
- Permissions change over time
- Old templates remain published
- No clear ownership

Copyright © 2026 Secure Ideas LLC

SecureIdeas professionally evil®

Legacy Services, Modern Problems

- Legacy enrollment services
- NTLM authentication
- Missing relay protections
- Security settings rarely revisited
- Unnecessary HTTP endpoints

Copyright © 2026 Secure Ideas LLC

What Should Administrators Be Doing?

- Enforce least privilege
- Review certificate templates regularly
- Limit unnecessary certificate capabilities
- Audit certificate issuance
- Secure legacy enrollment services
- Assign ownership and accountability

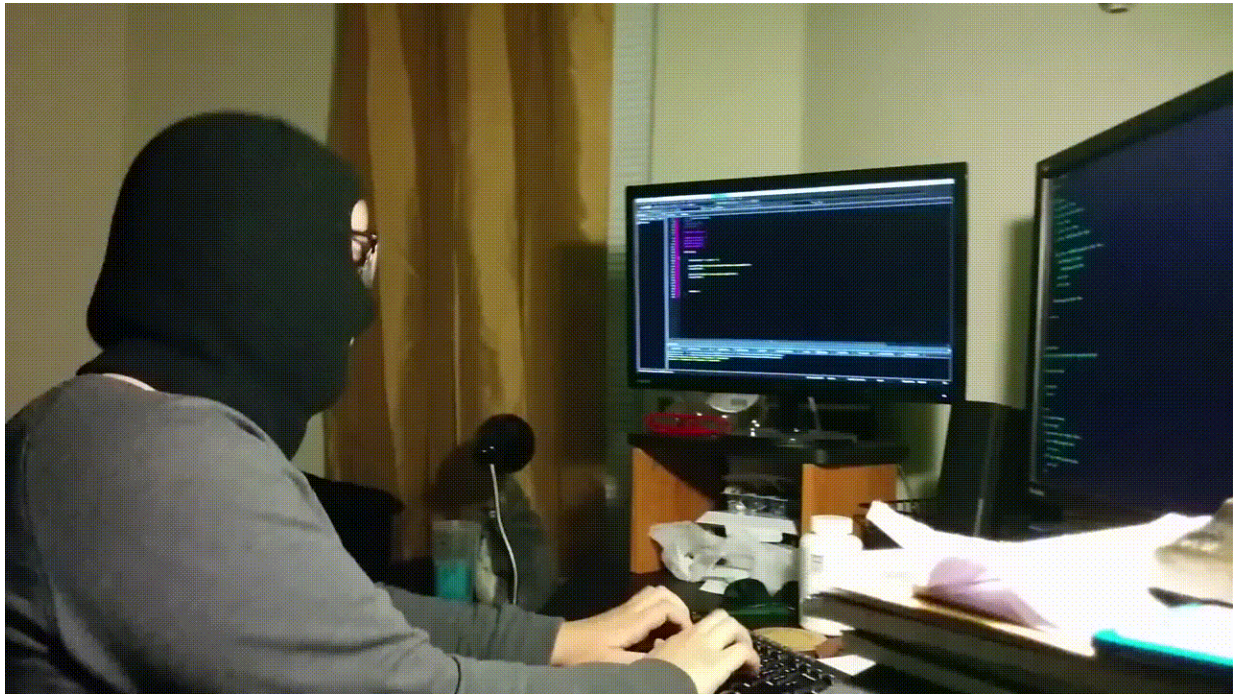
Copyright © 2026 Secure Ideas LLC

OR...



DON’T

And Let Us Keep Hacking



Q & A

866.404.7837
secureideas.com

Copyright © 2026 Secure Ideas LLC

professionally evil®