ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks
The Update Dilemma

When Trust Becomes the Attack Vector

Software updates were meant to be the safest moment in IT. A controlled change from a trusted source. A necessary ritual to keep systems secure and compliant. 'Patch early, patch often' was the gospel.

Today, that trust is under strain. Updates have become a paradox. Delay them and you stay exposed to known vulnerabilities. Apply them and you may be opening the door to something worse. Attackers have learned to exploit the update chain itself, abusing mechanisms like compromised successors, poisoned certificates, and vulnerable update services such as WSUS.

With updates capable of executing at high trust and spreading at scale, the question is no longer whether to update, but how to update safely without blindly trusting what runs at the heart of your infrastructure.

In this Threat Talks infographic we will discuss the following threats:

- Bad Successor
- WSUS RCE

32.1%
Nearly one-third of known exploited vulnerabilities were weaponized within 24 hours of disclosure.
Source: IT Pro

60%
of data breaches are tied to unpatched vulnerabilities.
Source: Wifi Talents

34%
of organizations say they are aware of vulnerablities before they are breached.
Source: GitNux

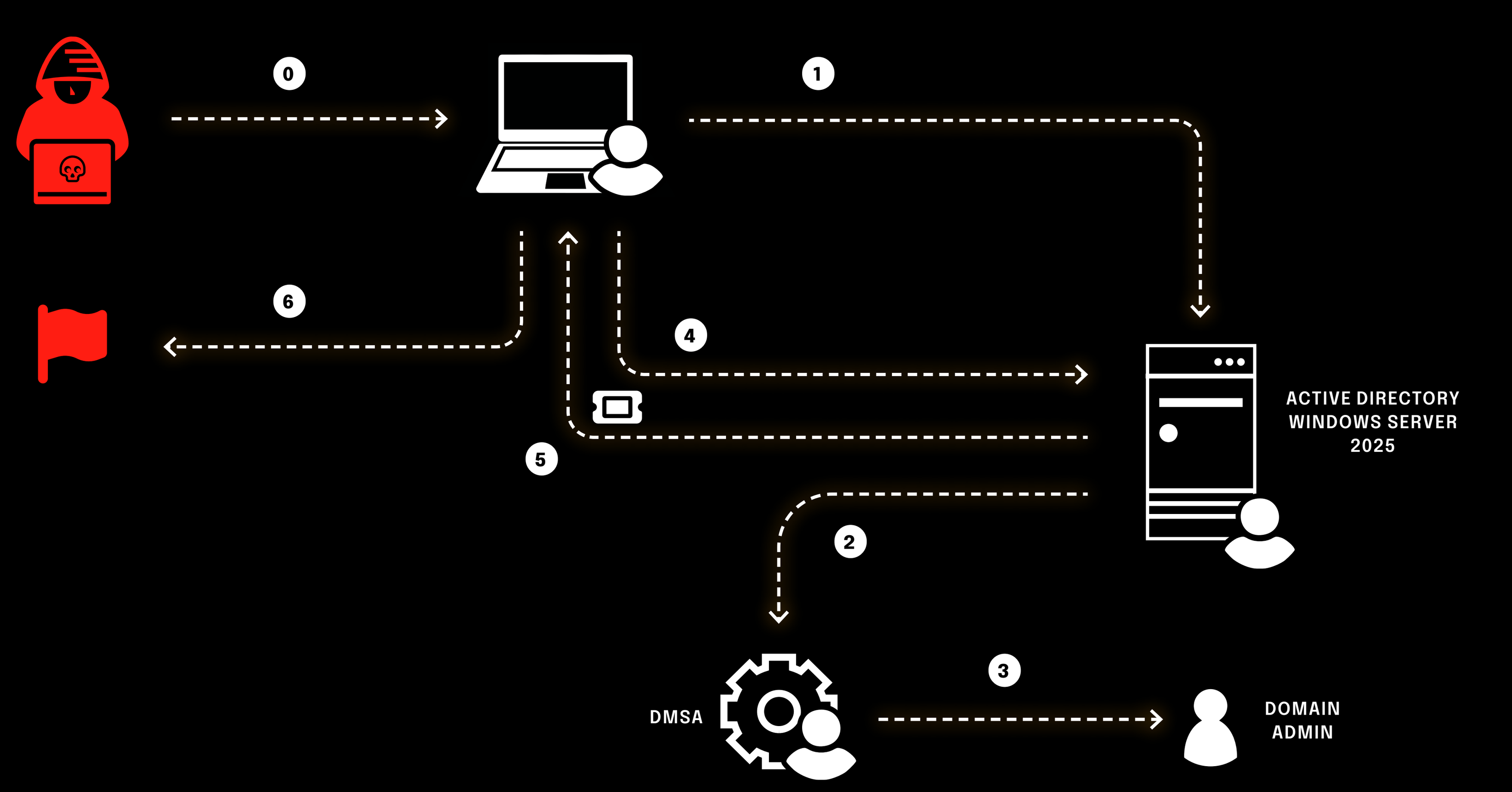
75%
Automated patching can eliminate 75% of exploitable vulnerabilities.
Source: Cyber Security News

Bad Successor

From "harmless permission" to full domain control

What if a perfectly legitimate Active Directory feature could quietly hand over Domain Admin privileges, without exploits, malware, or credential theft? BadSuccessor (CVE-2025-53779) does exactly that.

First disclosed in May-June 2025 (before receiving a CVE), BadSuccessor abuses delegated Managed Service Accounts (dMSAs) and normal AD migration logic. No memory corruption. No shellcode. Just design assumptions colliding with attacker creativity. Because it operates entirely within expected AD behavior, BadSuccessor can bypass many traditional detections that focus on group membership changes or credential theft, making it especially dangerous in mature, well-monitored environments.



0. Prerequisite

The attack relies on a specific but realistic set of conditions:

- A Windows Server 2025 Active Directory domain
- An attacker-controlled user account
- That account has Create Child Objects permissions
- A writable Organizational Unit (OU) where dMSAs can be created

These permissions are often granted for operational convenience and may not be considered high risk.

1. Interact with Domain Controller

The attacker communicates directly with the Domain Controller using standard AD interfaces.

- No exploit or abnormal protocol usage
- All actions appear legitimate from an AD perspective

2. Create dMSA Object in Writable OU

Using delegated permissions, the attacker:

- Creates a delegated Managed Service Account (dMSA)
- Places it in an OU where creation is allowed

At this stage, nothing appears suspicious – dMSAs are a supported and expected feature.

3. Point the dMSA to a Target Account

The attacker configures the dMSA to migrate from an existing account, typically a highly privileged one (e.g., Domain Admin).

- The migration is marked as "done"
- The dMSA inherits permissions from the original account
- No group memberships are changed on the original account

This is the core abuse: privilege inheritance without visible escalation.

4. Request a Kerberos Ticket

The attacker now requests a Kerberos service ticket for the newly created dMSA.

- This is a standard Kerberos operation
- No credentials of the original privileged account are required

5. Domain Controller Issues Kerberos Ticket

The Domain Controller:

- Validates the request
- Issues a Kerberos ticket tied to the dMSA
- The ticket reflects the effective privileges of the migrated account

From the DC's perspective, everything is working as designed.

6. Act with Mirrored Privileges

Armed with a valid Kerberos ticket:

- The attacker can act with the privileges of the original account
- Typically this results in full Domain Admin capabilities
- All without changing group membership or stealing credentials

At this point, the attacker has effectively *become* the target account.

Patch

- Install the August 2025 cumulative Windows updates
- These updates introduce mutual migration consent
- Marking migration as "done" on the dMSA alone is no longer sufficient
- The source account must also explicitly confirm the migration

This significantly raises the bar for abuse.

Mitigations and Defensive Measures

Reduce the Attack Surface

- Limit Create Child Objects permissions strictly
- Regularly review delegated permissions in OUs
- Remove permissions from accounts that do not explicitly require them

Protect Initial Access

- The attacker must already have a domain user and access to a domain-joined system
- Apply a protected surface and a Zero Trust Strategy to workstations and user accounts
- Enforce strong device and identity controls (e.g., tiering, PAWs)

CVE-2025-59287

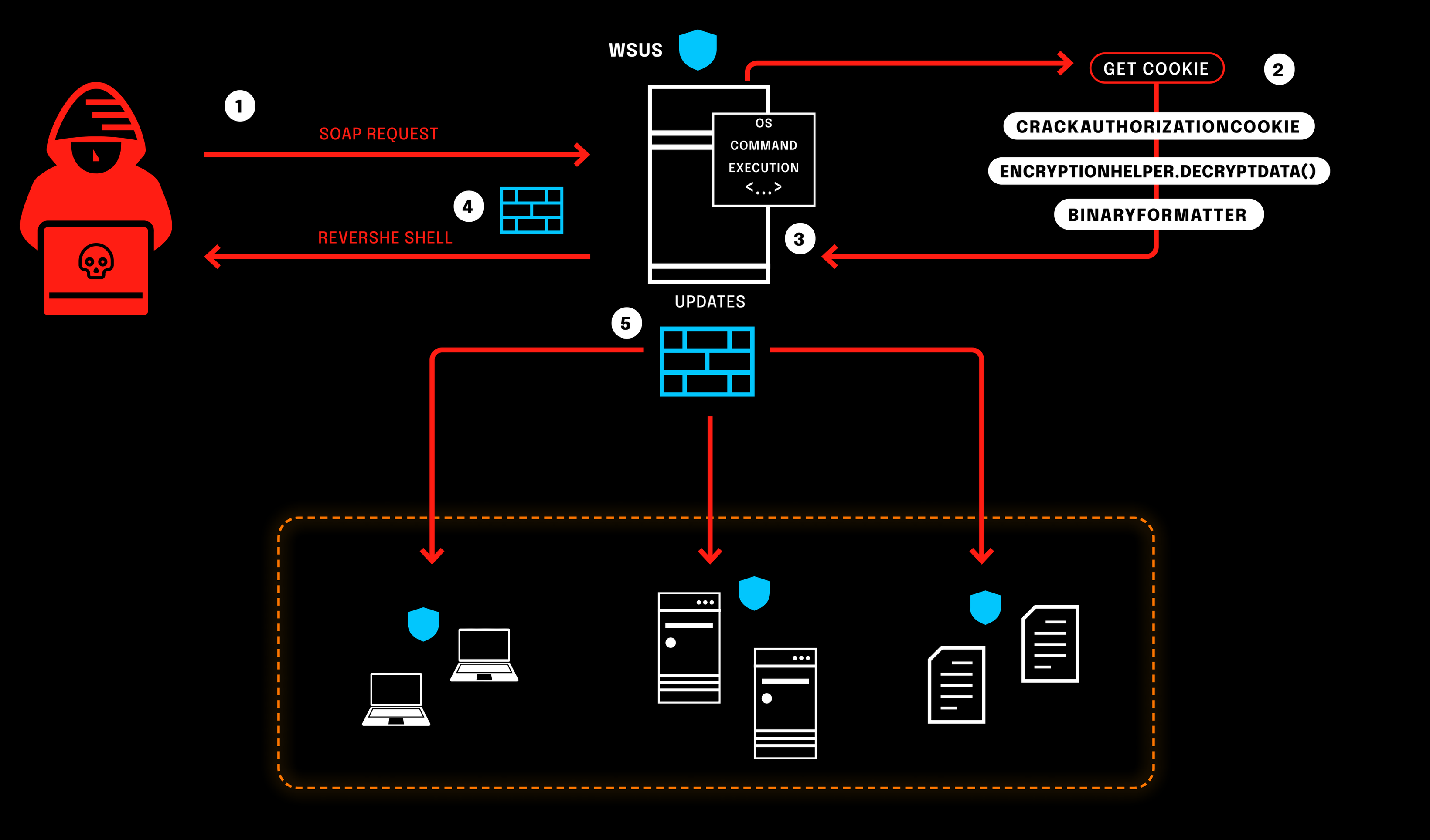
Remote Code Execution in Microsoft WSUS

On October 14, 2025, Windows Server Update Services (WSUS), a trusted internal patch-management service was revealed to contain a critical unauthenticated remote-code-execution vulnerability, tracked as CVE-2025-59287. This flaw allows a remote attacker to execute arbitrary code at SYSTEM privileges on vulnerable servers, and it has been actively exploited in the wild.

Severity Critical (CVSS 9.8)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1190 - Exploit Public-Facing Application	Exploit WSUS role via deserialization vulnerability → Remote SYSTEM code execution	Use default ports (8530/8531), exploit without credentials or user interaction	Low/Medium	Enterprises (servers with WSUS role exposed)

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1030 - Network Segmentation M1051 - Update Software M1047 - Audit	Public Facing Access (WSUS RCE)	Network monitoring, IOCs detection, BIOC rules	Critical	Advanced Persistent Threats / Cybercriminals



1. Malicious request

1. The attacker sends a specially crafted SOAP request to the WSUS GetCookie() endpoint at /ClientWebService/Client.asmx, embedding an encrypted malicious payload within the AuthorizationCookie.

M WSUS services should should not be directly exposed to internet. Internal access should be limited using strict firewall rules and network segmentation. Traffic to ports 8530/8531 should be tightly controlled and monitored.

2. Requests chain

2. The request passes through WSUS internals, where the encrypted payload is decrypted using a hardcoded AES key and sent directly to BinaryFormatter. Deserialize() without validation.

3. Code execution

3. Deserialization results in arbitrary code execution with SYSTEM-level privileges, allowing the attacker to run any command.

M EDR and XDR solutions should monitor for process injection and abnormal child processes. PowerShell or cmd.exe spawned from WSUS services is a red flag and must be investigated.

4. Reverse shell

4. At this point the attacker is able to execute tools like PowerCat using Invoke-Expression to establish a reverse shell for remote control.

M PowerShell logging must be enabled to detect encoded or obfuscated commands. Unusual outbound connections from WSUS servers should be flagged and blocked.

5. Post exploitation

5. As seen in the wild, Using tools like curl and certutil, the attacker downloads the ShadowPad malware and sideloads it via a legitimate executable (ETDCtrlHelper.exe) loading a malicious DLL (ETDApix.dll). From here the attacker can further expand in the network.

M Process behavior should be analyzed for signs of DLL sideloading. Use of certutil or curl on WSUS is highly suspicious. New services, scheduled tasks, or registry changes should trigger alerts.

Taxonomy

ATT&CK Technique
Which technique of the MITRE ATT&CK framework does the threat correspond to.

ATT&CK Mitigation
Which mitigation of the MITRE ATT&CK framework can be applied.

Attack Strategy
Plan devised by the attacker to exploit specific system vulnerabilities.

Attack Vector
What is the primary method of attack.

Evasion
Tactics used by the attacker to avoid detection or bypass security.

Detection
Mechanism to identify malicious activities or system anomalies.

Complexity
How easy it is to exploit the vulnerability or carry out the attack.

Threat Level
How severe the threat is.

Target Type
The category of organization that may potentially be targeted.

Threat Actor Type
What type of threat actor may be involved.

CONTACT US

mSOC score explanation:
We assign scores to both our sources and the news items. Sources are scored on a numeric scale ranging from 0 (untrustworthy) to 5 (verified), while news items are scored with a letter, ranging from E (unreliable) to A (reliable). By considering the scores of both the source and the news item and the quality of the available information, we classify the overall reliability into three categories: Confirmed, Verified, and Credible. Interested in learning more about our reliability scoring system for sources and news items? Our Threat Intelligence team would be happy to walk you through our procedure, so please don't hesitate to reach out.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS amsix