

从NTLM Relay看Windows RPC攻击面

文档仅限技术交流，切勿商用，违者必究



中安网星

Make Security Easy Again

分享人

中安网星高级安全专家——李帅臻

- ◆负责攻防对抗、漏洞研究、攻击建模、漏洞武器化等工作
- ◆专注于内网横向、域渗透在攻击场景中的利用
- ◆具备丰富的攻防实战经验
- ◆主要研究方向：Windows研究、内网高级攻击与防御、安全漏洞挖掘与利用等



目 录

01

• NTLM Relay

02

• RPC

03

• CVE-2022-30216

文档仅限技术交流，切勿商用，违者必究



NTLM Relay

文档仅限技术交流，切勿商用，违者必究



Printbug

The screenshot shows a Windows task manager window with the following processes listed:

| Pid | Protocol | Name |
|------|--------------|-------------------------|
| 1316 | ncacn_ip_tcp | 49163 |
| 1316 | ncacn_np | \pipe\spoolss |
| 1316 | ncalrpc | LRPC-dd5b1741a1393be077 |

The process details window shows the following information:

- Name: svchost.exe
- Pid: 892
- Image: 后台处理程序子系统应用
- Version: 6.3.9600.17415
- Path: C:\Windows\System32\spoolsv.exe
- CmdLine: C:\Windows\System32\spoolsv.exe
- User: NT AUTHORITY\SYSTEM
- Desktop:
- Image: 64-bits

The interface properties window shows the following information:

- Main
- RPC
- NDP

The decompilation window shows the following code:

```

2832 10B6EDBFA-4A24-4FC6-8A23-94281ECA65D11 1.0 RPC 7 Interpreted 0x00007f6ec833d20 0x00007f6ec800000 C:\Windows\System32\spoolsv.exe 0x1 后台处理程序子系统应用
2832 112345678-1234-ABCD-EF00-0123456789AB 1.0 RPC 118 Interpreted 0x00007f6ec800000 C:\Windows\System32\spoolsv.exe 0x1 后台处理程序子系统应用
2832 18970770-8664-11CF-9AF1-0000A56E724E 0.0 RPC 5 Interpreted 0x00007f6ec800000 C:\Windows\System32\combase.dll 0x21 用于 Windows 的 Microsoft COM
2832 14A452661-8290-4636-8F6E-7F4093A94678 1.0 RPC 4 Interpreted 0x00007f6ec833d20 0x00007f6ec800000 C:\Windows\System32\spoolsv.exe 0x1 后台处理程序子系统应用
2832 76F03F96-CDFO-44FC-A22C-64950A001209 1.0 RPC 75 Interpreted 0x00007f6ec833d20 0x00007f6ec800000 C:\Windows\System32\spoolsv.exe 0x1 后台处理程序子系统应用
    
```

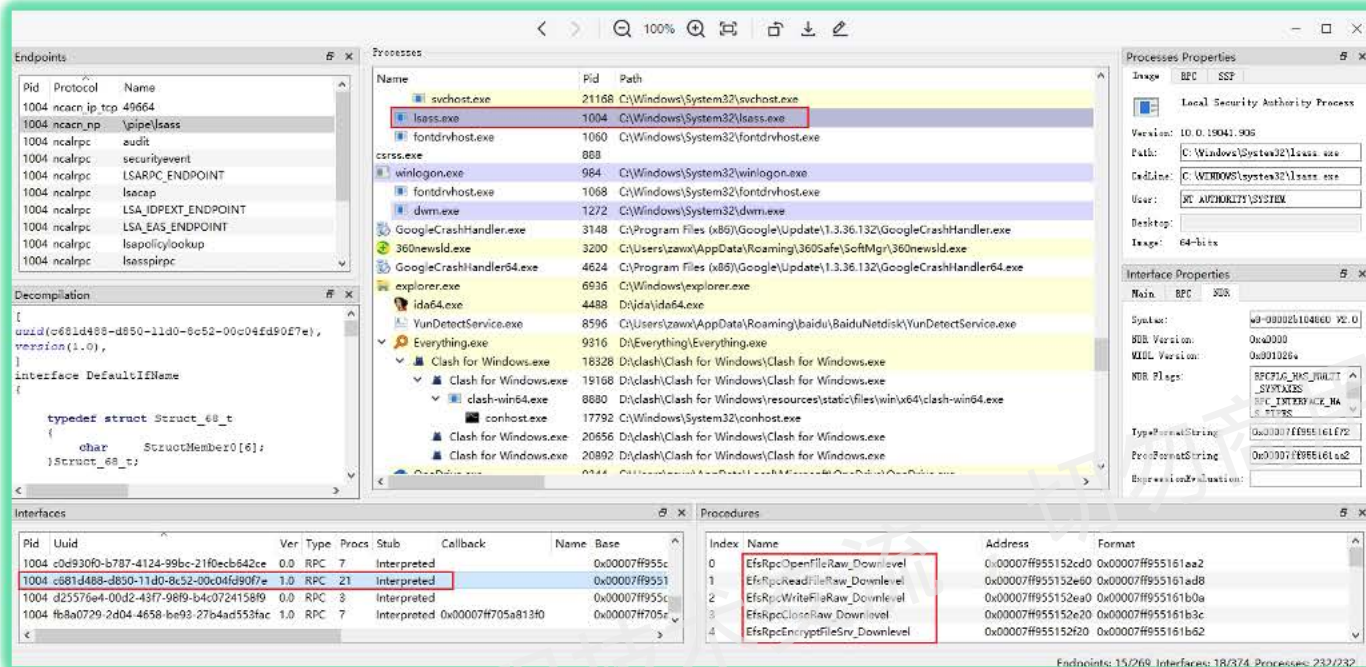
创建一个远程更改通知对象，该对象监视打印机对象的更改，并使用 () 将更改通知发送到打印客户端 RpcRouterReplyPrinter() 或 RpcRouterReplyPrinterEx。

```

DWORD RpcRemoteFindFirstPrinterChangeNotificationEx(
    [in] PRINTER_HANDLE hPrinter,
    [in] DWORD fdwFlags,
    [in] DWORD fdwOptions,
    [in, string, unique] wchar_t* pszLocalMachine,
    [in] DWORD dwPrinterLocal,
    [in, unique] RPC_V2_NOTIFY_OPTIONS* pOptions
);
    
```

pszLocalMachine：指向表示客户端计算机名称的字符串的指针。





用于打开服务器上的加密对象以进行备份或还原。它分配必须通过调用 EfsRpcCloseRaw 方法释放的资源。

```
long EfsRpcOpenFileRaw(
    [in] handle_t binding_h,
    [out] PEXIMPORT_CONTEXT_HANDLE* hContext,
    [in, string] wchar_t* FileName,
    [in] long Flags
);
```

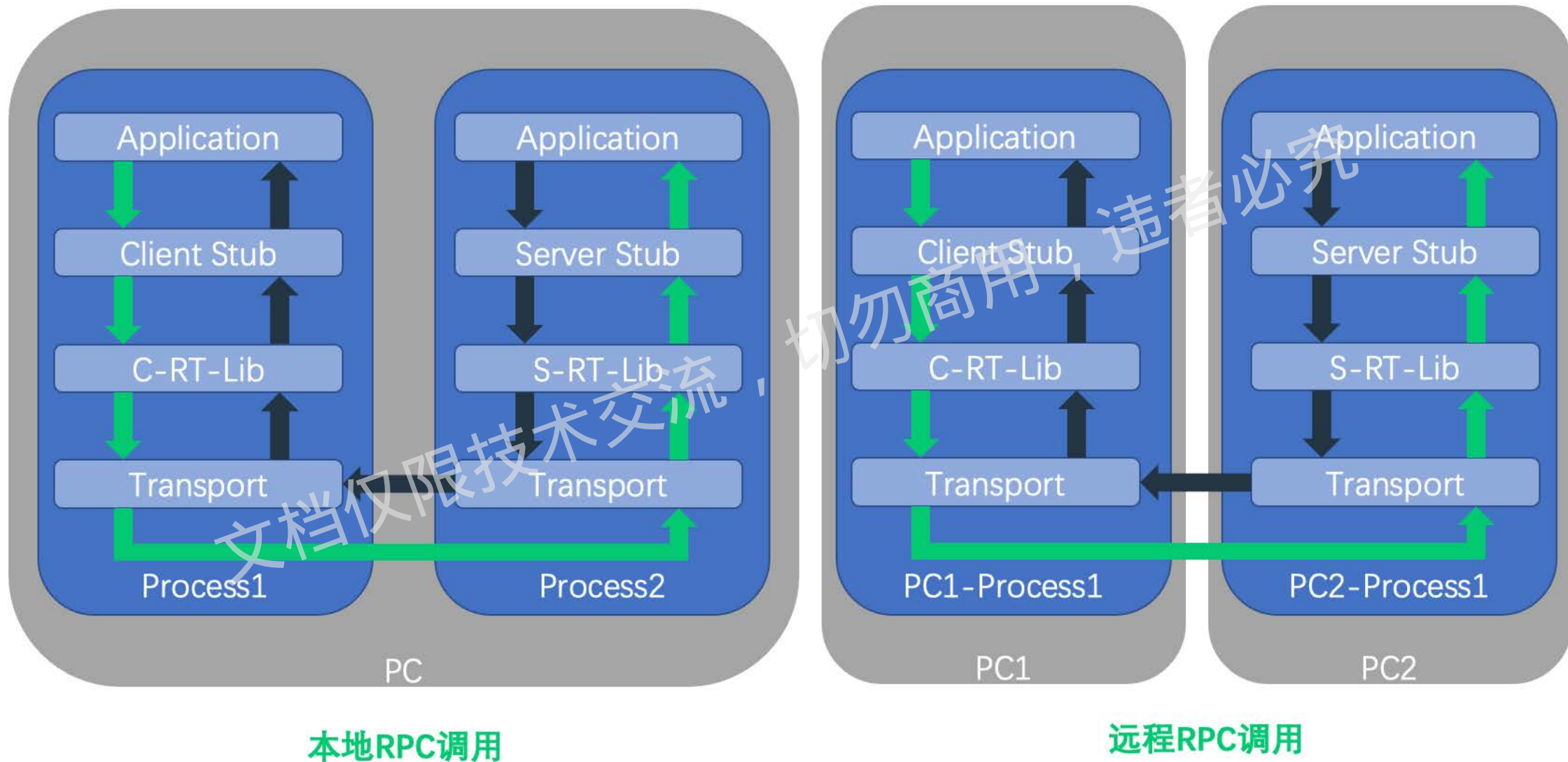
FileName：EFSRPC 标识符，指向远程服务器上的加密数据对象。应使用 Unc 路径作为 EFSRPC 标识符。



RPC

文档仅限技术交流，切勿商用，违者必究

RPC的两种调用方式



RPC应用场景

服务创建 (MS-SCMR)
目录复制服务 (MS-DRSR)
远程注册表 (MS-RRP)
计划任务 (MS-SCMR)
打印系统 (MS-RPRN)
Windows WMI (MS-WMI)
Netlogon 远程协议 (MS-NRPC)

The screenshot displays the Windows Task Manager and the Windows Management Instrumentation (WMI) console. The Task Manager window shows a list of processes, including `ServiceHub.VSDetouredHost.exe`, `services.exe`, `SgrmBroker.exe`, `ShellExperienceHost.exe`, `sihost.exe`, `smss.exe`, `spoolsv.exe`, `StartMenuExperienceHost.exe`, `svchost.exe`, and `svchost.exe`. The WMI console shows the `Interface Properties` for `Shell Infrastructure Host`, including the `Version` (10.0.19041.746), `Path` (`C:\Windows\System32\sihost.exe`), `CmdLine` (`sihost.exe`), `User` (`DESKTOP-7BDKQKA\zawx`), `Desktop`, `Image` (64-bits), and `Interface Properties` (Main, RPC, NDR). The `Interface Properties` section includes the `Syntax` (`68-080021104860 V2.0`), `NDR Version` (`0x0000`), `WIDL Version` (`0x01026e`), `NDR Flags` (`RPCPLG_HAS_MULTIPLE_SYNTAXES`, `RPC_INTERFACE_HAS_FTPES`), `TypeFormatString` (`0x00007f927aee5aa`), `ProcFormatString` (`0x00007f927aee3f2`), and `ExpressionEvaluation`.

| Pid | Protocol | Name |
|------|----------|-------------------------|
| 5048 | ncalrpc | OLE67CFD155ABD97EDDB8 |
| 5048 | ncalrpc | LRPC-e6640d0b5f9bfb1b66 |

| Name | Pid | Path |
|-------------------------------|------|---|
| ServiceHub.VSDetouredHost.exe | 8384 | C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\ServiceHub\Hosts\ServiceHub.Host.AnyC |
| services.exe | 952 | |
| SgrmBroker.exe | 7824 | |
| ShellExperienceHost.exe | 2908 | C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2xyewy\ShellExperienceHost.exe |
| sihost.exe | 5048 | C:\Windows\System32\sihost.exe |
| smss.exe | 696 | |
| spoolsv.exe | 3532 | |
| StartMenuExperienceHost.exe | 8136 | C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2xyewy\StartMenuExperienceH |
| svchost.exe | 1032 | |
| svchost.exe | 1152 | |
| svchost.exe | 1196 | |
| svchost.exe | 1292 | |
| svchost.exe | 1408 | |
| svchost.exe | 1512 | |
| svchost.exe | 1556 | |
| svchost.exe | 1564 | |
| svchost.exe | 1608 | |
| svchost.exe | 1624 | |
| svchost.exe | 1660 | |
| svchost.exe | 1692 | |
| svchost.exe | 1720 | C:\Windows\System32\svchost.exe |
| svchost.exe | 1768 | |

| Pid | Uuid | Ver | Type | Procs | Stub | Callback | Name | Base |
|------|--------------------------------------|-----|------|-------|-------------|-------------------|-------------------|------|
| 6176 | 0820a0d0-1aee-49f9-acf9-3e3d3fe303cb | 2.0 | RPC | 40 | Interpreted | 0x00007f92934d650 | 0x00007f92934d650 | |
| 1720 | 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd | 1.0 | RPC | 14 | Interpreted | 0x00007f92934d650 | 0x00007f92934d650 | |
| 5048 | 0fc77b1a-95d8-4a2e-a0c0-cff54237462b | 0.0 | RPC | 9 | Interpreted | 0x00007f927aa5740 | 0x00007f927aa5740 | |
| 5048 | 18f70770-8e64-11cf-9af1-0020af6e72f4 | 0.0 | RPC | 5 | Interpreted | 0x00007f927aa5740 | 0x00007f927aa5740 | |

| Index | Name | Address | Format |
|-------|--|-------------------|-------------------|
| 0 | FmMuxSrvRegisterFGNotificationCoreUIEndpoint | 0x00007f927acafa0 | 0x00007f927aee3f2 |
| 1 | FmMuxSrvUnRegisterFGNotificationCoreUIEndpoint | 0x00007f927acbf00 | 0x00007f927aee422 |
| 2 | FmMuxSrvGetForegroundProductId | 0x00007f927acabe0 | 0x00007f927aee452 |
| 3 | FmMuxSrvIsForegroundProductId | 0x00007f927acae00 | 0x00007f927aee482 |
| 4 | FmMuxSrvGetProductIdFromProcessId | 0x00007f927acac30 | 0x00007f927aee4b8 |

Endpoints: 75/75 Interfaces: 87/87 Processes: 234/234

国内外对RPC研究方向

← 推文



Compass Security
@compassecurity

NTLM Relay over RPC: our analyst Sylvain Heiniger @sploutchy explored new attack vectors and discovered a vulnerability in the Windows Task Scheduler.



Ophir Harpaz
@OphirHarpaz

Yesterday, @nachoskrnl and I presented some of the research that has been going on in our team on MS-RPC. Long story short, Ben found a new auth coercion vulnerability on which you can read here akamai.com/blog/security/... I'd like to highlight a couple more things from the talk.
>>

← 推文



Ophir Harpaz
@OphirHarpaz

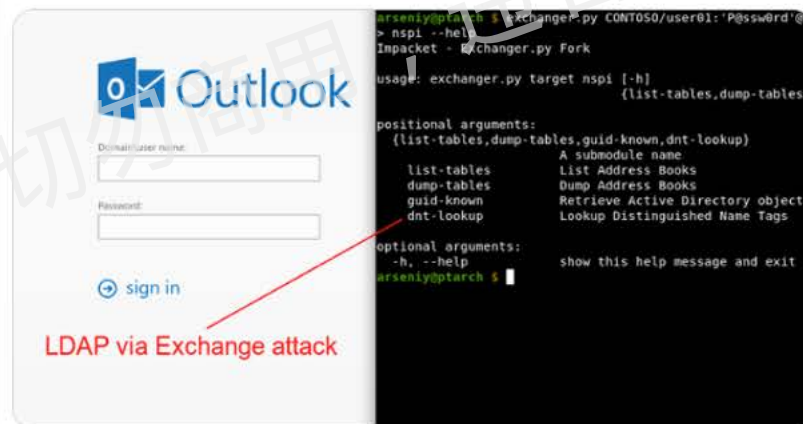
Everyone's talking about the 9.8 RCE bug in Windows RPC runtime (CVE-2022-26809). @nachoskrnl bin-diffed rpcrt4.dll and located the integer overflow that was patched. Read about it here - akamai.com/blog/security/... Patch now, and ffs don't expose TCP 445 to the internet.



PT SWARM
@ptswarm

New attack! Our researcher Arseniy Sharoglazov has discovered a method to connect to LDAP via #MSExchange from the Internet and access the whole Active Directory database. Read the research: swarm.ptsecurity.com/attacking-ms-e...

翻译推文



Jonas Vestberg
@bugch3ck

回复 @ikarlslund

My bet is something exposed over MS-RPC. That attack surface is huge and fairly unexplored. But I wouldn't be surprised if it was Exchange again 😊 (even though I would not consider it "Windows system").

RPC分析工具

Wireshark packet capture details for a DCE/RPC request.

Frame 1478: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits) on interface \Device\NPF_{F3CE4818-022F-488F-BC23-F9647D18E3B0}, id 0

Ethernet II, Src: VMware_a4:a8:8a (00:50:56:a4:a8:8a), **Dst:** VMware_a4:5f:f9 (00:50:56:a4:5f:f9)

Internet Protocol Version 4, Src: 192.168.16.250, **Dst:** 192.168.16.249

Transmission Control Protocol, Src Port: 50123, **Dst Port:** 49670, **Seq:** 2237, **Ack:** 352, **Len:** 540

Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, FragLen: 540, Call: 2837, Ctx: 0, [Resp: #1483]

Version: 5
Version (minor): 0
Packet type: Request (0)
Packet Flags: 0x03
Data Representation: 10000000 (Order: Little-endian, Char: ASCII, Float: IEEE)
Frag Length: 540
Auth Length: 76
Call ID: 2837
Alloc hint: 432
Context ID: 0
Opnum: 3
[Response in frame: 1483]
Auth Info: Kerberos SSP, Packet privacy, AuthContextId(0)
DRSUAPI, DsGetNCChanges

Wireshark
RPCView
RPCDump
PortQry

Processes window showing running processes and their paths.

| Name | Pid | Path |
|---------------------------|------|---|
| ZhuDongFangYu.exe | 3124 | |
| svchost.exe | 3176 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3364 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3452 | C:\Windows\System32\svchost.exe |
| spoolsv.exe | 3532 | C:\Windows\System32\spoolsv.exe |
| svchost.exe | 3624 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3632 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3672 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3956 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4104 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4112 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4120 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4128 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4140 | C:\Windows\System32\svchost.exe |
| OneApp.IGCC.WinService... | 4172 | C:\Windows\System32\DriverStore\FileRepository\igcc_dch.inf_amd64_9cf4db1af1d1b22d\OneApp.IGCC.WinSe |
| WavesSysSvc64.exe | 4224 | C:\Windows\System32\DriverStore\FileRepository\wavesapo9de.inf_amd64_e99a314c3593d5e7\WavesSysSvc64 |
| RstMwService.exe | 4236 | C:\Windows\System32\DriverStore\FileRepository\viatorac.inf_amd64_42f9d9bf72d84cf\RstMwService.exe |
| RtkAudUService64.exe | 4244 | C:\Windows\System32\DriverStore\FileRepository\realtekservice.inf_amd64_a1020546271138b9\RtkAudUService |
| RtkAudUService64.exe | 6500 | C:\Windows\System32\DriverStore\FileRepository\realtekservice.inf_amd64_a1020546271138b9\RtkAudUService |
| WifiAutoInstallSvc.exe | 4256 | C:\Program Files (x86)\TP-LINK\TL-WDN5200免驱版 2.0\AutoInstSvc\WifiAutoInstallSvc.exe |

Interfaces window showing network interfaces.

| Pid | Uuid | Ver | Type | Procs | Stub | Callback | Name | Base |
|------|--------------------------------------|-----|------|-------|-------------|-------------------|---------------|------|
| 3532 | 0b6edbf4-4a24-4fc6-8a23-942b1eca... | 1.0 | RPC | 7 | Interpreted | 0x00007f664807b90 | 0x00007f6647d | |
| 3532 | 12345678-1234-abcd-ef00-01234567... | 1.0 | RPC | 118 | Interpreted | 0x00007f6647d | 0x00007f6647d | |
| 3532 | 18f70770-8e64-11cf-9af1-0020af6e72f4 | 0.0 | RPC | 5 | Interpreted | 0x00007f6647d | 0x00007f6647d | |
| 3532 | 4a452661-8290-4b36-8fbc-7f4093a9... | 1.0 | RPC | 4 | Interpreted | 0x00007f664807b90 | 0x00007f6647d | |

Procedures window showing RPC procedures.

| Index | Name | Address | Format |
|-------|-------------------------|--------------------|--------------------|
| 0 | _UseProtseq | 0x00007f6647d47c0 | 0x00007f6647d47c0 |
| 1 | _GetCustomProtseqInfo | 0x00007f6647d44b0 | 0x00007f6647d44b0 |
| 2 | _UpdateResolverBindings | 0x00007f6647d318b0 | 0x00007f6647d318b0 |
| 3 | _NotifyFDI | 0x00007f6647d4790 | 0x00007f6647d4790 |
| 4 | _ControlTracing | 0x00007f6647d2cb10 | 0x00007f6647d2cb10 |

Processes Properties window showing details for the selected process (svchost.exe).

Version: 10.0.19041.746
Path: C:\Windows\System32\svchost.exe
CmdLine: C:\WINDOWS\System32\svchost.exe
User: NT AUTHORITY\SYSTEM
Desktop:
Image: 64-bits

Interface Properties

Main **RPC** **NDR**

Syntax: w8-080023104860 V2.0
NDR Version: 0xa0000
NDR Flags: 0x001020e
NDR Flags: RPC_INTERFACE_HUS_F
TYPES
TypeFormatString: 0x00007f6647d47c0
ProcFormatString: 0x00007f6647d47c0
ExpressionEvaluation:

Endpoints: 4/270 Interfaces: 6/375 Processes: 234/234

RPC参数详解

- Interfaces
- Interface UUID
- Opnum
- Procedures
- Endpoints
- RPC protocol sequence

The screenshot displays the Process Hacker tool interface, showing the 'Processes' list, 'Endpoints' list, 'Decompilation' window, 'Interfaces' list, and 'Procedures' list.

Endpoints:

| Pid | Protocol | Name |
|------|--------------|-----------------------|
| 3532 | ncacn_ip_tcp | 49669 |
| 3532 | ncacn_np | \pipe\spoolss |
| 3532 | ncalrpc | LRPC-ac1c5db3ff1e30ed |
| 3532 | ncalrpc | OLED2049825FE79BE3B |

Processes:

| Name | Pid | Path |
|---------------------------|------|---|
| ZhuDongFangYu.exe | 3124 | |
| svchost.exe | 3176 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3364 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3452 | C:\Windows\System32\svchost.exe |
| spoolsv.exe | 3532 | C:\Windows\System32\spoolsv.exe |
| svchost.exe | 3624 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3632 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3672 | C:\Windows\System32\svchost.exe |
| svchost.exe | 3956 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4104 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4112 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4120 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4128 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4140 | C:\Windows\System32\svchost.exe |
| OneApp.IGCC.WinService... | 4172 | C:\Windows\System32\DriverStore\FileRepository\igcc_dch.inf_amd64_9cf4db1af1fd1b22d\OneApp.IGCC.WinSe |
| WavesSysSvc64.exe | 4224 | C:\Windows\System32\DriverStore\FileRepository\wavesapo9de.inf_amd64_e99a314c3593d5e7\WavesSysSvc64 |
| RstMwService.exe | 4236 | C:\Windows\System32\DriverStore\FileRepository\iastorac.inf_amd64_42f9d9bfb72d84c\RstMwService.exe |
| RtkAudUService64.exe | 4244 | C:\Windows\System32\DriverStore\FileRepository\realtekse.inf_amd64_a1020546271138b9\RtkAudUService |
| RtkAudUService64.exe | 6500 | C:\Windows\System32\DriverStore\FileRepository\realtekse.inf_amd64_a1020546271138b9\RtkAudUService |
| WifiAutoInstallSvc.exe | 4256 | C:\Program Files (x86)\TP-LINK\TL-WDN5200免驱版 2.0\AutoInstSvc\WifiAutoInstallSvc.exe |

Decompilation:

```

error_status_t Proc1_GetCustomi
[in]short arg_1,
[in][size_is(arg_1)]short a
[out][ref]struct Struct_30_

error_status_t Proc2_UpdateResc
[in]struct Struct_30_t* arg_
[in][out]hyper *arg_3,
[out][ref]struct Struct_30_
[out][ref]struct Struct_30_

error_status_t Proc3_NotifyFDT

```

Interfaces:

| Pid | Uuid | Ver | Type | Procs | Stub | Callback | Name | Base |
|------|--------------------------------------|-----|------|-------|-------------|--------------------|----------------|------|
| 3532 | 0b6edbf4-4a24-4fc6-8a23-942b1eca... | 1.0 | RPC | 7 | Interpreted | 0x00007ff664807b90 | 0x00007ff6647d | |
| 3532 | 12345678-1234-abcd-ef00-01234567... | 1.0 | RPC | 118 | Interpreted | 0x00007ff664807b90 | 0x00007ff6647d | |
| 3532 | 18f70770-8e64-11cf-9af1-0020af6e72f4 | 0.0 | RPC | 5 | Interpreted | 0x00007ff956d19ed0 | 0x00007ff956c4 | |
| 3532 | 4a452661-8290-4b36-8f8e-7f4093a9... | 1.0 | RPC | 4 | Interpreted | 0x00007ff664807b90 | 0x00007ff6647d | |

Procedures:

| Index | Name | Address | Format |
|-------|-------------------------|--------------------|--------------------|
| 0 | _UseProtseq | 0x00007ff956df47c0 | 0x00007ff956ee10c2 |
| 1 | _GetCustomProtseqInfo | 0x00007ff956df44b0 | 0x00007ff956ee1104 |
| 2 | _UpdateResolverBindings | 0x00007ff956d318b0 | 0x00007ff956ee113a |
| 3 | _NotifyFDT | 0x00007ff956df4790 | 0x00007ff956ee1176 |
| 4 | _ControlTracing | 0x00007ff956d2cb10 | 0x00007ff956ee11a0 |

Processes Properties:

Image: 后台处理程序子系统应用
Version: 10.0.19041.746
Path: C:\Windows\System32\spoolsv.exe
CmdLine: C:\WINDOWS\System32\spoolsv.exe
User: NT AUTHORITY\SYSTEM
Desktop:
Image: 64-bits

Interface Properties:

Main: RPC NDR
Syntax: e8-08002b104860 V2.0
NDR Version: 0xa0000
MIDL Version: 0x801026a
NDR Flags: RPC_INTERFACE_MAS_IPES
TypeFormatString: 0x00007ff956ee11d2
ProcFormatString: 0x00007ff956ee10c2
ExpressionEvaluation:

Endpoints: 4/270 Interfaces: 6/375 Processes: 234/234

RPC调用分析

| Pid | Uuid | Ver | Type | Procs | Stub | Callback | Name | Base |
|------|--------------------------------------|-----|------|-------|-------------|-------------------|---------------|------|
| 3532 | 0b6edbfa-4a24-4fc6-8a23-942b1eca... | 1.0 | RPC | 7 | Interpreted | 0x00007f664807b90 | 0x00007f6647d | |
| 3532 | 12345678-1234-abcd-ef00-01234567... | 1.0 | RPC | 118 | Interpreted | 0x00007f664807b90 | 0x00007f6647d | |
| 3532 | 18f70770-8e64-11cf-9af1-0020af6e72f4 | 0.0 | RPC | 5 | Interpreted | 0x00007f664807b90 | 0x00007f6647d | |
| 3532 | 4a452661-8290-4b36-8fbc-7f4093a9... | 1.0 | RPC | 4 | Interpreted | 0x00007f664807b90 | 0x00007f6647d | |

```
[
  uuid(18f70770-8e64-11cf-9af1-0020af6e72f4),
  version(0.0),
]
interface DefaultIfName
{
    typedef struct Struct_30_t
    {
        short StructMember0;
        short StructMember1;
        [size_is(StructMember0)]short StructMember2[];
    }Struct_30_t;

    error_status_t Proc0__UseProtseq(
        [in]short arg_1,
        [in][unique][string] wchar_t* arg_2,
        [out]long *arg_3,
        [out][ref]struct Struct_30_t** arg_4,
        [out][ref]struct Struct_30_t** arg_5);

    error_status_t Proc1__GetCustomProtseqInfo(
        [in]short arg_1,
        [in][size_is(arg_1)]short arg_2[],
        [out][ref]struct Struct_30_t** arg_3);

    error_status_t Proc2__UpdateResolverBindings(
        [in]struct Struct_30_t* arg_2,
        [in][out]hyper *arg_3,
        [out][ref]struct Struct_30_t** arg_4,
        [out][ref]struct Struct_30_t** arg_5);
}
```

| Constant/value | Description |
|--|--|
| ncacn_nb_tcp Connection-oriented NetBIOS over Transmission Control Protocol (TCP) | Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT |
| ncacn_nb_ipx Connection-oriented NetBIOS over Internet Packet Exchange (IPX) | Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT |
| ncacn_nb_nb Connection-oriented NetBIOS Enhanced User Interface (NetBEUI) | Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows Me, Windows 98, Windows 95 |
| ncacn_ip_tcp Connection-oriented Transmission Control Protocol/Internet Protocol (TCP/IP) | Client only: MS-DOS, Windows 3.x, and Apple Macintosh Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows Me, Windows 98, Windows 95 |
| ncacn_np Connection-oriented named pipes | Client only: MS-DOS, Windows 3.x, Windows 95 Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT |
| ncacn_spx Connection-oriented Sequenced Packet Exchange (SPX) | Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows Me, Windows 98, Windows 95 |
| ncacn_dnet_nsp Connection-oriented DECnet transport | Client only: MS-DOS, Windows 3.x |
| ncacn_at_dsp Connection-oriented AppleTalk DSP | Client: Apple Macintosh Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT |
| ncacn_vms_spp Connection-oriented Vines scalable parallel processing (SPP) transport | Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT |
| ncadg_ip_udp Datagram (connectionless) User Datagram Protocol/Internet Protocol (UDP/IP) | Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT |
| ncadg_ipx Datagram (connectionless) IPX | Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT |
| ncadg_mq Datagram (connectionless) over the Microsoft Message Queue Server (MSMQ) | Client only: Windows Me/98/95 Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT Server 4.0 with SP3 and later |
| ncacn_http Connection-oriented TCP/IP using Microsoft Internet Information Server as HTTP proxy | Client only: Windows Me/98/95 Client and Server: Windows Server 2003, Windows XP, Windows 2000 |
| ncalrpc Local procedure call | Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows Me, Windows 98, Windows 95 |

UUID

IDL

RPC protocol sequence

RPC相关漏洞



- Potato
- ZeroLogon
- PrinterNightMare





CVE-2022-30216

文档仅限技术交流，切勿商用，违者必究

RpcView

File Options View Filter Help

Endpoints

| Pid | Protocol | Name |
|------|----------|-------------------------|
| 4468 | ncacn_np | \PIPE\svrsvc |
| 4468 | ncalrpc | LRPC-79ab057ee3b018fbb6 |

Decompilation

```
[  
  uuid(c681d488-d850-11d0-8c52-00c04fd90f7e),  
  version(1.0),  
]  
interface DefaultIfName  
{  
  typedef struct Struct_68_t  
  {  
    char StructMember0[6];  
  }Struct_68_t;  
}
```

Processes

| Name | Pid | Path |
|----------------------------|------|---|
| svchost.exe | 4468 | C:\Windows\System32\svchost.exe |
| vmware-authd.exe | 4568 | C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe |
| svchost.exe | 4576 | C:\Windows\System32\svchost.exe |
| svchost.exe | 4584 | C:\Windows\System32\svchost.exe |
| vmware-usbarbitrator64.exe | 4656 | C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe |
| svchost.exe | 4744 | C:\Windows\System32\svchost.exe |
| jhi_service.exe | 5000 | C:\Windows\System32\DriverStore\FileRepository\dal.inf_amd64_31a8dbbf39dcdc3b\jhi_ser |
| svchost.exe | 5352 | C:\Windows\System32\svchost.exe |
| svchost.exe | 5556 | C:\Windows\System32\svchost.exe |
| svchost.exe | 5972 | C:\Windows\System32\svchost.exe |
| svchost.exe | 6220 | C:\Windows\System32\svchost.exe |
| svchost.exe | 6324 | C:\Windows\System32\svchost.exe |
| svchost.exe | 6444 | C:\Windows\System32\svchost.exe |
| svchost.exe | 6568 | C:\Windows\System32\svchost.exe |
| svchost.exe | 6808 | C:\Windows\System32\svchost.exe |
| dasHost.exe | 5704 | C:\Windows\System32\dasHost.exe |
| svchost.exe | 7008 | C:\Windows\System32\svchost.exe |
| svchost.exe | 7064 | C:\Windows\System32\svchost.exe |
| svchost.exe | 7132 | C:\Windows\System32\svchost.exe |
| ctfmon.exe | 6308 | C:\Windows\System32\ctfmon.exe |

Processes Properties

Image: RPC

Windows 服务主进程

Version: 10.0.19041.546

Path: C:\Windows\System32\svchost.exe

CmdLine: C:\WINDOWS\system32\svchost.exe

User: NT AUTHORITY\SYSTEM

Desktop:

Image: 64-bits

Interface Properties

Main RPC NDR

Syntax: a8-08002b104860 V2.0

NDR Version: 0xa0000

MIDL Version: 0x801026e

NDR Flags: RPCFLG_HAS_MULTIPLE_SYNTAXES, RPC_INTERFACE_HAS_MULTIPLE_SYNTAXES

TypeFormatString: 0x00007ff9347bece2

ProcFormatString: 0x00007ff9347bfe22

ExpressionEvaluation:

Interfaces

| Name | Base | Location | Flags | Description | EpMapper | Anr |
|------|--------------------|---------------------------------|-------|----------------------------|------------|-----|
| 0 | 0x00007ff8efa10000 | C:\Windows\System32\ssdpsrv.dll | 0x1 | SSDP 服务 DLL | Registered | |
| 0 | 0x00007ff9550f0000 | C:\Windows\System32\sspsrv.dll | 0x21 | LSA SSPi RPC interface DLL | | |
| 0 | 0x00007ff935680000 | C:\Windows\System32\stpsvc.dll | 0x21 | 提供使用安全套接字隧道协议(SS... | | |
| 0 | 0x00007ff8f0c80000 | C:\Windows\System32\StorSvc.dll | 0x21 | 存储服务 | Registered | |
| 0 | 0x00007ff8f0c80000 | C:\Windows\System32\StorSvc.dll | 0x29 | 存储服务 | Registered | |

Procedures

| Index | Name | Address | Format |
|-------|-------------------------------------|--------------------|--------------------|
| 69 | LocalAliasGet | 0x00007ff9347a4d20 | 0x00007ff9347c0d16 |
| 70 | LocalServerCertificateMappingGet | 0x00007ff9347af390 | 0x00007ff9347c0d4e |
| 71 | LocalServerCertificateMappingAdd | 0x00007ff9347aea40 | 0x00007ff9347c0da4 |
| 72 | LocalServerCertificateMappingEnum | 0x00007ff9347aee30 | 0x00007ff9347c0de2 |
| 73 | LocalServerCertificateMappingRemove | 0x00007ff9347af7f0 | 0x00007ff9347c0e26 |
| 74 | NetServerTransportAddForInstance | 0x00007ff9347ab320 | 0x00007ff9347c0e5e |

Endpoints: 2/273 Interfaces: 378/378 Processes: 239/239

历史版本实现

IDA View-A Pseudocode-A Hex View-1 Structures

```

1 int64 __fastcall SsRpcSecurityCallback(RPC_IF_HANDLE InterfaceUuid, void *Context)
2 {
3     unsigned int v3; // ebx
4     RPC_WSTR StringBinding; // [rsp+30h] [rbp-A8h] BYREF
5     RPC_WSTR Protseq; // [rsp+38h] [rbp-A0h] BYREF
6     RPC_BINDING_HANDLE ServerBinding[2]; // [rsp+40h] [rbp-98h] BYREF
7     int RpcCallAttributes[2]; // [rsp+50h] [rbp-88h] BYREF
8     char v9[52]; // [rsp+58h] [rbp-80h] BYREF
9     int v10; // [rsp+8ch] [rbp-4ch]
10    __int6 v11; // [rsp+A8h] [rbp-30h]
11
12    StringBinding = 0i64;
13    Protseq = 0i64;
14    memset_0(v9, 0, 0x68ui64);
15    RpcCallAttributes[0] = 2;
16    RpcCallAttributes[1] = 96;
17    if ( RpcServerInqCallAttributes(Context, RpcCallAttributes)
18        || (unsigned __int16)(v11 - 64) <= 5u && v10 != 1
19        || (unsigned __int16)(v11 - 58) <= 5u && v10 != 1 && !(unsigned __int8)SsIsCallerClusterAccount()
20        || RpcBindingServerFromClient(Context, ServerBinding) )
21    {
22        return S164;
23    }
24    if ( RpcBindingToStringBindingW(ServerBinding[0], &StringBinding)
25        || (v3 = RpcStringBindingParseW(StringBinding, 0i64, &Protseq, 0i64, 0i64, 0i64)) != 0
26        || !stricmp(Protseq, L"ncacn_np") )
27    {
28        v3 = 5;
29    }
30    RpcBindingFree(ServerBinding);
31    if ( StringBinding )
32        RpcStringFreeW(&StringBinding);
33    if ( Protseq )
34        RpcStringFreeW(&Protseq);
35    return v3;
36 }
    
```

Line 1 of 456

Graph overview

00000410 SsRpcSecurityCallback:1 (180001010)

Windows 10 19H2

File Edit Jump Search View Debugger Options Windows Help

IDA View-A Pseudocode-A Strings Hex View-1 Structures

```

1 int64 __fastcall SsRpcSecurityCallback(RPC_IF_HANDLE InterfaceUuid, void *Context)
2 {
3     unsigned int v3; // ebx
4     RPC_WSTR StringBinding; // [rsp+30h] [rbp-A8h] BYREF
5     RPC_WSTR Protseq; // [rsp+38h] [rbp-A0h] BYREF
6     RPC_BINDING_HANDLE ServerBinding[2]; // [rsp+40h] [rbp-98h] BYREF
7     int RpcCallAttributes[2]; // [rsp+50h] [rbp-88h] BYREF
8     char v9[52]; // [rsp+58h] [rbp-80h] BYREF
9     int v10; // [rsp+8ch] [rbp-4ch]
10    __int6 v11; // [rsp+A8h] [rbp-30h]
11
12    StringBinding = 0i64;
13    Protseq = 0i64;
14    memset_0(v9, 0, 0x68ui64);
15    RpcCallAttributes[0] = 2;
16    RpcCallAttributes[1] = 96;
17    if ( RpcServerInqCallAttributes(Context, RpcCallAttributes)
18        || (unsigned __int16)(v11 - 64) <= 9u && v10 != 1
19        || (unsigned __int16)(v11 - 58) <= 5u && v10 != 1 && !(unsigned __int8)SsIsCallerClusterAccount()
20        || RpcBindingServerFromClient(Context, ServerBinding) )
21    {
22        return S164;
23    }
24    if ( RpcBindingToStringBindingW(ServerBinding[0], &StringBinding)
25        || (v3 = RpcStringBindingParseW(StringBinding, 0i64, &Protseq, 0i64, 0i64, 0i64)) != 0
26        || !stricmp(Protseq, L"ncacn_np") )
27    {
28        v3 = 5;
29    }
30    RpcBindingFree(ServerBinding);
31    if ( StringBinding )
32        RpcStringFreeW(&StringBinding);
33    if ( Protseq )
34        RpcStringFreeW(&Protseq);
35    return v3;
36 }
    
```

Line 1 of 1

Graph overview

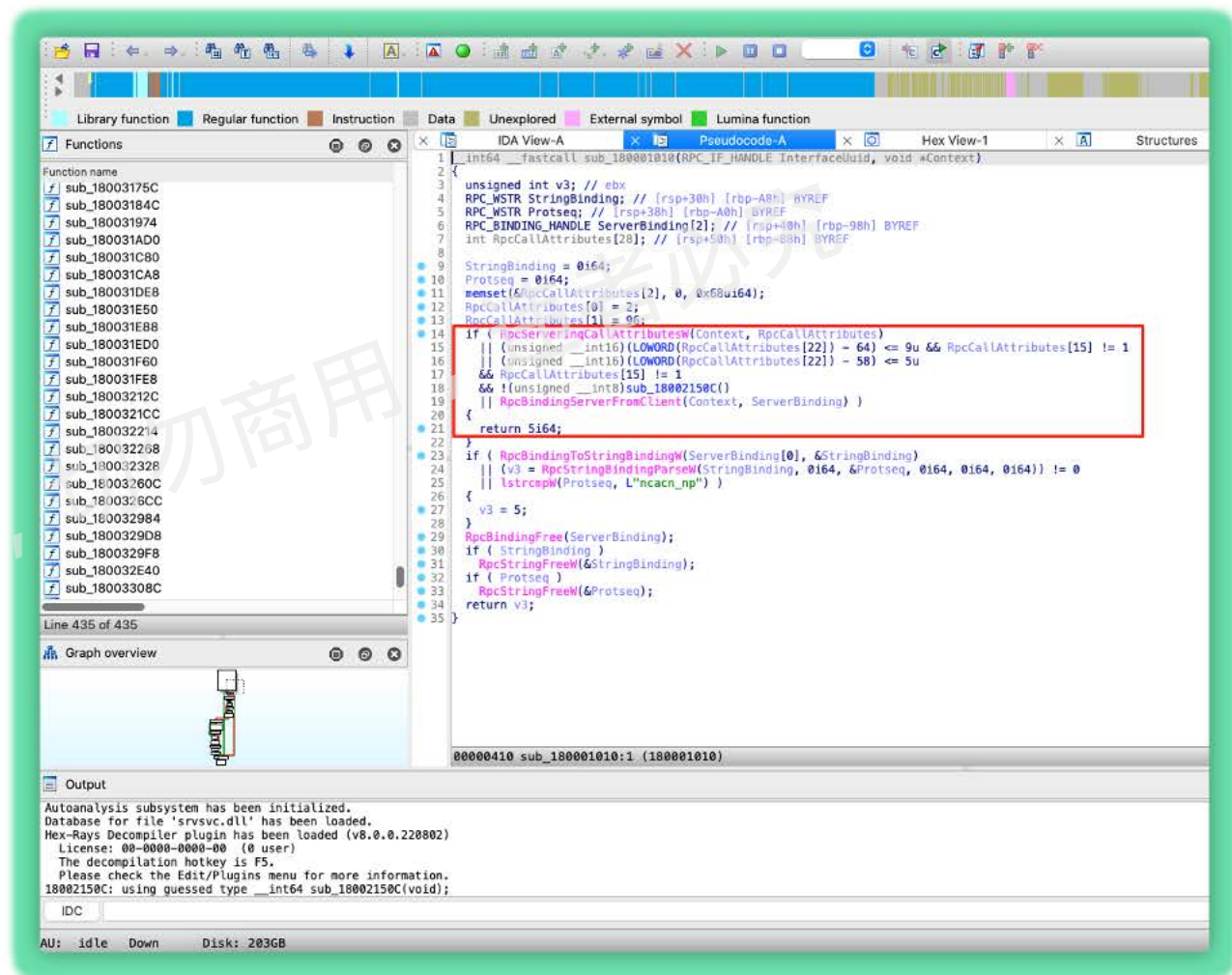
00000474 SsRpcSecurityCallback:17 (180001074)

Windows 10 20H2

漏洞分析

```
.rdata:00007FFEEE276670 dq offset LocalrServerCertificateMappingGet
.rdata:00007FFEEE276678 dq offset LocalrServerCertificateMappingAdd
.rdata:00007FFEEE276680 dq offset LocalrServerCertificateMappingEnum
.rdata:00007FFEEE276688 dq offset LocalrServerCertificateMappingRemove
.rdata:00007FFEEE276690 dq offset LocalrServerCertificateMappingModify
```

```
LocalrServerCertificateMappingModify(
    [in, string, unique] SRVSVC_HANDLE ServerName,
    [in] long arg_1,
    [in][out][switch_is(arg_1)] union certificate_container* arg_2
);
```



Windows 11/Server 2022

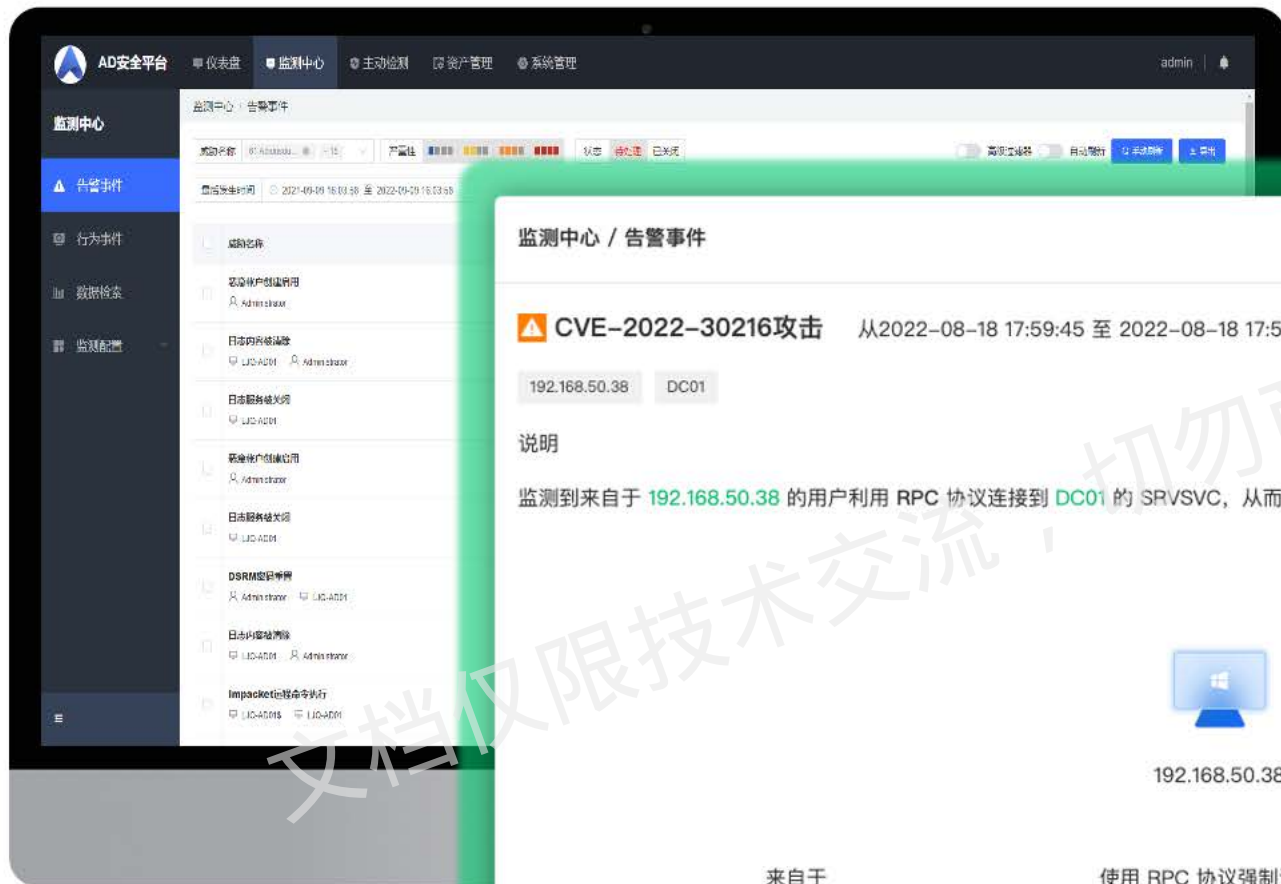

```
~
+ python3 cve-2022-38126.py
[-] Connecting to endpoint
[+] Connected
[+] Binding to uuid
[+] Successfully bound
[-] Try LocalServerCertificateMappingModify
[+] Got Handle
[+] Complete
~
+
```

```
[-] Setting up Smb Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] SMBD-Thread-5: Received connection from 192.168.16.249, attacking target http://192.168.16.250
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://192.168.16.250 as TEST16/DC01$ SUCCEED
[*] SMBD-Thread-7: Connection from 192.168.16.249 controlled, but there are no more targets left!
[*] SMBD-Thread-8: Connection from 192.168.16.249 controlled, but there are no more targets left!
[*] SMBD-Thread-9: Connection from 192.168.16.249 controlled, but there are no more targets left!
[*] SMBD-Thread-10: Connection from 192.168.16.249 controlled, but there are no more targets left!
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 36
[*] Base64 certificate of user DC01$:
MIIRFIQIBAzCCEtCGCSqGSIb3DQEHAcCEGgEhEKMIIIRIDCCB1cGCqGSIb3DQEHAcCEGgEhEKMIIHPQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQhwQgQIRJA1oQ6S3VoY
CaggAgIIEHEaHF+vxhy1Krf0LJNfPNYw3IwhmjsBnIrowZHXtXhVFG1Kw6m1P0S0L1VQYm1bhi1eltafU9gpzMQVJurrZakA7hg9J7srg5qZJJGUZxmg1WQbM4X0Z5QE1
2fgJQ94a5f9a21dBRyyJ1Cu08mF3GP0fZbhbYsk7WqD27CtjQhJ48538Tq84f1c3j24uokD0056swCBM9UVbyBQkpHDDLvtfFpGSUBUdndSfML7Gm+jjE3oe8K98SxwKJ
7001g5F35n6agWjZ7H6KcYFT+/eVIZTbRwTsT1caffYKnpLMATCGMV9HykM3/1gL4-JGtNd/kPiE8RIBOR07fwU/ks5mVvswJgkV7bDzxoJ8mAq/P7LsdffwZIZU/ok08uKd
03mmqhKQK804dpd+RTRVVB1I9a11P2z2m031b1pGpH1x2X11C1FohWog/8b+mqgqIrxJwCoF7CWPTksGroEr6QGRKL8kJAaGvG/Ha+Q1ugs5H0wBzNS4uo5J1i9uD6J9w
0XVnNtNIihj/r0/rB9cWtBp7z5MDocnE6S1nc4aghhZEPde6FK174G14+85buJ+Fkw9680QXZLuv8G/PjYsk2haF1jg7yqQydsE00pUeYzaz2RA2FXgzaAaf+Y7bVA1z
3F7/fN0Lo1GUn1ND6N1X0bnKkL0px/seQ07R6dePhDPFJZ035d593ntVJQr7g40q97/AM7h5y96tCM0AfgaKGoKqbmVdzUgRSGsp18r3CEJPQANET1m30n5o+1i11ybMyXR
Dt001GU7o6VQADH1096LYXkav/vyLUVpghk+FSdeUpumYUSE9Qn7N8b3ztJHJ3VneY8grkH39138pKzLhwa8RU1xWMS5cVnkjIc4ExXPr07Xpext9jpbTSb1UE1LzgoW
pG1edqGqVHW+89IFX/hALMQRdnKcom9KgzCDV+b257NmW7Vx3bQJ2Dgoh9xzn20+uL1WUpFQCmK53JcEoDIRufeo2ESCV0BHePebPM8LEy00/sbRMOu3/ZUE3p3GtX2ZU/
3uv8Bu7oTouzZapbx0YeutGhpqgJu15xELxzgIHWMLYInDgWfG9AenE1vFkgk0zL15q8ARQXaKut/HWLi1AA5F8VYocpcvXnRPmwwGNDVgD3XFbGy1+PLfzPFPUBHdy2L0
Hsyolo46VrsowKk74EK1xiEnxPDh0Ct/Vmdjicla1/ezevBduogzPpajUS0YFxa4QLedmkvq1tFu9uGyHzrgTgAQ0VFEFNJlUgQk3/KMDGq1B36vu+GUNg5dhk0MB/5CKYUa9m
001KsKv40LcmgPtK+b5Kw+QtZKhY/CKsq1FZCYFTXoYTPQWJea09fVzPmtL/C/CG1Vd5weamGLAR1B3/XbXWYU360qz33pa7KAQ4J9o792zNSQUZtE0bwbw8LW1VnPn+8ndQ
y1f4Tb0tYek5YwmN8m0SIL0ev7HSbulnMap1XV1M87T1DwaMRkAPYas21nnTA9331GdF1zdkKhrvSV/Rk1I7i+DRVAASMAR1Vdr2vS1sq+HXRg3x2gTmUclUq8nPVbJk6rRQ
dkXUkujFW3ArkF657/5die05x61+WpajwZQM/
Q9EVurNFK39pSiZiJf80Wd/sdtKRA0HMF0
s219h13JYDu9TCEhJN1JeJ+fs14LVFKQSto
u6/JaSE2FegPKHTfFN5J+qB0x3TFP0mn9CEUA
5KlcSVqeJL+UwG9N7FQnaJVM06tLLrthSzy44
BmffqIA11ZnI95TbQJod6sxnLp265n/19F+Is
oZIHvNAQCBoI1JsgSCC4wggnqMIJpgYLKo
FSVEbdMyiYe04sKFxG+hCTMCr0e9D5n1wto65
euG6fHsQv777kmbU315K5AW17BuzIZcLjcs/
GSbX6VjvndyU+Mqjam1SUYNd851AKnManMjme
R75+WhJb5u0fallC03pPVJCFc66s1fkmUpP/CE
7L+H+J5sU2z2kfs9h08VQ2PwfrU5n4cyKrqQL
3kv73wyTGhUhtXgLFCHcgF8Lx5bokhocad5Jc
t40uQowQ/uG0JCOH6GWXQvSRtgPwHxZ2Wce
h1CpEEvK0EeyQyRSfp/ZtMmQ0Xhgx+9SfUnn
F+okQMBUg7vzVAnPmAWsLTLBvzLmJR+1rk1KcnZHx6u7HEPTXfalCqxID6Ur3+onjbtGGFYpt2/4e4zhJyDvdMA7Wgc+n4b3+GhzjKTxDtTectvIRV5aF15wY3K3R72G1qG15
J2T4M0Giz+Uffu2D0qgaUgK4IDrfr3532NXJwX3XVgZUGn0n52Acars+q+k/Aj+ucmhLeX6Hw/Rv8YrCJ0cNH53bJDXTL6SNN1jtbuuuuu+xyY8TaJ1c+3hu7oeJ0QSA1Y0
FKAZJup46b0KXmF+lvqIKU6kGQ22Za10LgmYQP84ewE0b11uutos8j/aG0F5VPEUheCdtS1mGhYwcbF05ZF5R8x+PpDS1/z1/7GEKenV9L/bhvj26AMVb8m1G5G5xjQxQe0b
BGoTv2160TEwmI0f4Xyww52vPt9trshvLmGZvf/HscB7AYGEKvWQEFtFbTUUXf0PezX7on5CGIOCMrGuLj50nkr7P1Z1DnrElt4D0JNnElisQabktWrdEIAV9ekJQ11oASWx
dLXUfQ061Rj1VWGWGoW01m1XBWMPvPmFnpT0F4H+4s321XgZ4FLSEgio1ZtPm8AM0h6Ct/Y9v4xGmchScf351eGuYrLUCK0K1Z/AGW2w0FK16TFUUn491dh4d4cTG6R8J/hn
U1+0/EsJcJZh628QsGH5jZC0L0tDa79YWCb+eihwX0D9TU+Jg805615u0qct70u73sCN0VIAaMDY21jo/mQnxIT77qNRjFPmu9I7m/cDxCvsbsKbV922W04ybXnaNTLJWgW
bTID0b/Hu+o4t3k5yURTxgb/lke2M11b/1fQh2s79CFpbI69bmgAnLLH6d6d1TW69P5WFP0z1XaFxyI38YNQK5U1pnc0V87vGZLhASALUBPKPqh7z30dqK4e39316Z1YPUhQy
wa3G5ayj2zXMuIQuY33F8dEckMkyVEPL/kAD+C0CTZ3vE75EytTaLcQQuim/qMhsAor7Egm0L1TXv53MMVn2rMucPsrP1zmhbqHhKcYwuA1EechKux0MfRF2j4BSUXFLU1j/
28EPS1phTUN0FCk72nJn60TureV/f18VNYz6JmyEYCjgvXQRiId+uH7Z2L61nJAYJUSJC5shdw9aCdoXyAaysG9yztQ9hassC2FrgIKWhGKqC57Q3e3mVPJY254xb/U1j/
GernA94IS2LAgQzQVQC3G02sAK6T+dw/RCLuE8jQ/21RfnDaFGInsuKJw+6RnRKTmaoKw4dxbE+aggAQ1r7KbSAAK4CLBwOR1xy19ME4ecvnnDHHfEHx+8dKgt1Cnk76V5OCrc
Ppu3tx8kL2T8rUaL0iuzFFWAgV+9n1Kpw1S1HDKRSEF4wWp1NF1q8jK05wZES1ie40OYSUwzJM/JDLz4JzUIQBH1TVF11zGzhqDboB41z/mE85X0VWHLu0kzq35tWkN1L5pJ
beLatbc/zG+XU/4VnzjRVXo0C3n865s/aV08AJDdA9q5oku1ej73269UHNC0K56eoe8nMw96j9meID62W9xjVc10XFpjjYXnz1S19LjE36mF83R1pxvMFcn8HVCgH5oCeaG6e
4Gbs7T53ePZ36X/Kc9TtyjzcLZBwqAnQ8fXwM01otrPdWMePb8T1uLKjbb88MjVqZLZx54p1RCfE7IVmDmqgFP22oaTeSCWzBamXbd3S0ZBxw2UTVjWSm1rdkktccf9D9n+W
nU1U/8YohaptVx273Xcu/CqkqAt+Rn8aE0a1ekU0w5phM72a5pZTDf5JNhbFuIA0hIJQFG0H07V0nHecazyn3WLCJSLndZGGA938GChE+zBfJ0K6KzrH4a0a0eX9or8Jb
ZUY8R6dvaaXovQ7EPA1x14szmZQT6TNTUpCCcY2rEJXBt4ROSJX0Z/ZIUYGld/HT+/P3wyZ2NGyGht30gZCLyUsRbCFF1CCT5G8Cacvbnffe5ajzlaqHoVJ3zh4d0c71eXcFTx
y7w0PPXod0X6b6Jn24TrgXDRM/xx7f356AxJTAjBgkqhkiG9w0BCRUxFQUSZvFXhs1p3S1maewjVaeqYGM/fwPTAXMAGCWCGSALAwQCAQUABCC+dmmQ1jZ375SwjrcQ0+DH
FHU0uGwEwGwvESKUFvjFwQ1LrG1cUTFKhg=
```

文档仅限技术交流，

攻击监测



监测中心 / 告警事件

CVE-2022-30216攻击

从2022-08-18 17:59:45 至 2022-08-18 17:59:45

横向移动

待处理

操作

192.168.50.38

DC01

说明

监测到来自于 192.168.50.38 的用户利用 RPC 协议连接到 DC01 的 SRVSVC，从而导致目标服务器向任意服务器发起 NTLM 身份验证请求。



192.168.50.38



DC01

来自于

使用 RPC 协议强制认证

连接到任意服务器并执行 NTLM 身份验证

证据

导出

THANK YOU

文档仅限技术交流，切勿商用，违者必究