This document will hold information for both protocols: MS-RPRN & MS-PAR due to similarities in activity and usage.

Protocol:

- Print System Remote Protocol (MS-RPRN)
- Print System Asynchronous Remote Protocol (MS-PAR)

Interface UUID:

- 12345678-1234-ABCD-EF00-0123456789AB (MS-RPRN) (synchronous)
- 76F03F96-CDFD-44FC-A22C-64950A001209 (MS-PAR- IRemoteWinspool Interface) (asynchronous)

Server Binary:

- spoolsv.exe

Endpoint:

- ncacn_np: `\pipe\spoolss` (MS-RPRN)
- ncacn_ip_tcp (dynamic endpoint) (MS-PAR)

ATT&CK Relation:

- Privilege Escalation
- Print Nightmare
- Printer Bug
- T1210 - Exploitation of Remote Services
- T1547.012 - Print Processors

Indicator of Activity (IOA):

- Print Nightmare:
  - Network:
  - Methods:
    - MS-PAR / `RpcAsyncAddPrinterDriver()`
    - MS-RPRN / `RpcAddPrinterDriverEx()`
- Host:
  - File created: `C:\Windows\System32\spool\drivers\(x64/W32X86)\*\*.dll`

    - Transfers/Loads a driver: `C:\Windows\System32\spool\drivers\(x64/W32X86)\*\*.dll`
    - Queries: `HKLM\Software\Policies\Microsoft\Windows NT\Printers` & `HKLM\System\CurrentControlSet\Control\Print\Environments\Windows x64\Drivers\Version-3\Microsoft enhanced Point and Print compatibility driver\*`
        - Set SACL on registry key within test environment and there didn't seem to be a lot of noise.
    - Registry Create: `HKLM\System\CurrentControlSet\Control\Print\Environments\Windows x64\Drivers\Version-*\*.dll` (x64 bit systems) / `HKLM\SYSTEM\CurrentControlSet\Control\Print\Environments\Windows NT x86\*.dll` (x86 bit systems)
    - 5156 - Inbound connection to spoolsv.exe over (pipe or tcp) from weird machines
    - `spoolsv.exe` spawns a process.

- "The Printer Bug" vulnerability/Spool Service:
    - Network:
        - SMB activity over named pipe: `\pipe\spoolss`
        - Methods:
            - `RpcRemoteFindFirstPrinterChangeNotification`
            - `RpcRemoteFindFirstPrinterChangeNotificationEx`
    - Host:
        - Watch for 5145 events where domain controllers are being accessed via `IPC$` share through named pipe - `\pipe\spoolss`
        - Extra suspicious if activity is coming from domain controllers outside of current domain

- Both:
    - If Spooler is turned off/disabled - detection to trigger when it is enabled/turned back on.

Prevention Opportunities:

- Print Nightmare:
    - Microsoft patch
        - Set all values to zero, if they exist in environment:
            - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
            - `NoWarningNoElevationOnInstall = 0` (DWORD) or not defined (default setting)
            - `UpdatePromptSettings = 0` (DWORD) or not defined (default setting)
            - If `NoWarningNoElevationOnInstall = 1`, system is vulnerable
        - Turn off Spooler Service if possible, disable from starting back up on boot
        - Disable Spooler from accepting client connections (GPO setting)
        - Adjust `RestrictDriverInstallationToAdministrators` registry value to prevent non-administrators from installing printer drivers on a print server
        - RPC filters to make sure only a certain group has access to perform RPC method
        - Disable Point and Print in the registry: `reg add ""HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint"" /v Restricted /t REG_DWORD /d 0 /f`

- Printer Bug:
    - Turn off Spooler Service if possible, disable from starting back up on boot
    - Disable kerberos delegation where possible
    - Disable Spooler from accepting client connections (GPO setting)
    - Enable Account is sensitive and cannot be delegated for high privileged accounts

- Both:
    - RPC Filter Example:

```
rpc
filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=12345678-1234-A
add condition field=remote_user_token matchtype=equal data=D:(A;
add condition field=auth_level matchtype=equal data=6
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=12345678-1234-A
add filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=76F03F96-CDFD-4
add condition field=remote_user_token matchtype=equal data=D:(A;
add condition field=auth_level matchtype=equal data=6
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=76F03F96-CDFD-4
add filter
quit
```

    - Filter will only allow Domain Admins to communicate over interface `12345678-1234-ABCD-EF00-0123456789AB` & `76F03F96-CDFD-44FC-A22C-64950A001209`, where the authentication level is `RPC_C_AUTHN_LEVEL_PKT_PRIVACY (6)`. This is to prevent potential relay attacks from happening.
    - If you don't want to assign DA's to this DACL, so it might be best to create a Printer specific group or change it to Local Admins (BA).

Notes:

- Service Name: Spooler
- Methods must specify object UUID: `9940CA8E-512F-4C58-88A9-61098D6896BD`
- "The Printer Bug" was created by Lee Christensen and can be used to force authentication and extract the TGT of the target domain controller.
- Print Nightmare (CVE-2021-1675) is a vulnerability that allows remote code execution to any workstation/server with the Spooler service enabled.
- Adding RPC Filter, but honestly the best course of action is to disable spooler where possible. Could always overlap these prevention strategies. Aka - Turn off/Disable spooler, set RPC filter in the case someone turns it back on, and write detection logic for Spooler being turned on.
- If RPC filter is applied, suggest creating a specific user and not DA to limit DA logins

Useful Resources:

- https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory
- https://www.sygnia.co/demystifying-the-printnightmare-vulnerability
- https://github.com/leechristensen/SpoolSample