Sign in

jsecurity101 / MSRPC-to-ATTACK Public

Notifications Fork 40 Star 307

Code Issues Pull requests Actions Projects Security Insights

MSRPC-to-ATTACK / documents / MS-EFSR.md

jsecurity101 Adding DFSNM 1872e5c · 2 years ago

154 lines (126 loc) · 6.06 KB

Preview Code Blame Raw

Protocol:

- Encrypting File System Remote (EFSRPC) Protocol - (MS-EFSR)

Interface UUID:

- `c681d488-d850-11d0-8c52-00c04fd90f7e` (unauthenticated implementation)
- `df1941c5-fe89-4e79-bf10-463657acf44d`

Server Binary:

- `efslsaext.dll` (loads into) `lsass.exe`(unauthenticated implementation)
- `efssvc.dll` (loads into) `lsass.exe`

Endpoint:

- ncacn_np: `\\pipe\lsass` alias `\\pipe\lsarpc` (unauthenticated implementation)
- ncacn_np: `\\pipe\efsrpc`

ATT&CK Relation:

- T1187 - Forced Authentication
- PetitPotam

Indicator of Activity (IOA):

PetitPotam:

- Network:
  - Inbound network connection over port 445
  - Connection over pipe `lsarpc` or `lsass` (`lsarpc` is points to lsass)
  - Connection over pipe `efsrpc`
  - Methods:
    - `EfsRpcOpenFileRaw` (patched by Microsoft via CVE-2021-36942)
    - `EfsRpcEncryptFileSrv`
    - `EfsRpcDecryptFileSrv`
    - `EfsRpcQueryUsersOnFile`
    - `EfsRpcQueryRecoveryAgents`
    - `EfsRpcRemoveUsersFromFile`
    - `EfsRpcAddUsersToFile`
- Host:
  - (Server Side + Attack came from non-domain joined host):
    - Event ID 5145 on Target:
      - `ANONYMOUS LOGON`
      - Account Domain: `NT AUTHORITY`
      - Object Type: `File`
      - Share Name: `\\*\IPC$`
      - Relative Target Name: `lsarpc`

            - Access Mask: `0x3`
            - Accesses:
                - `ReadData (or ListDirectory)`
                - `WriteData (or AddFile)`
        - Event ID 4624 on Target:
            - Logon Type: `3`
            - Account Name: `Anonymous Logon`
            - Account Domain: `NT SECURITY`
            - Logon Process: `NtLmSsp`
- For version where the source host is a domain joined host, the data will be similar except 4624 logon will be a domain user over NTLM. Join LogonID from 4624 with LogonID on 5145

CVE-2021-43893:

- Network:
    - Inbound network connection over port 445
    - Connection over pipe `efsrpc`
    - Methods:
        - `EfsRpcOpenFileRaw`
        - `EfsRpcEncryptFileSrv`
        - `EfsRpcCloseRaw`
        - `EfsRpcReadFileRaw`
        - `EfsRpcEncryptFileSrv`
- Host:
    - (Server Side):
        - Event ID 5145 on Target:
            - Account Name: domain user
            - Object Type: `File`
            - Share Name: `\\*\IPC$`

        - Relative Target Name: `efsrpc`
        - Access Mask: `0x12019F`
        - Accesses:
            - `READ_CONTROL`
            - `SYNCHRONIZE`
            - `ReadData (or ListDirectory)`
            - `WriteData (or AddFile)`
            - `AppendData (or AddSubdirectory or CreatePipeInstance)`
            - `ReadEA`
            - `WriteEA`
            - `ReadAttributes`
            - `WriteAttributes`
    - Event ID 4624 on Target:
        - Logon Type: `3`
        - Account Name: domain user
        - Process ID: `0x0`
        - Elevated Token: `Yes`
    - Sysmon EID 11 on Target:
        - FileName: Name of newly created file

- Join on LogonID for queries.
- Wouldn't be uncommon to see multiple events if the attacker was creating a directory and uploading a file.

Prevention Opportunities:

- Apply MSFT Patch (Read: https://tiraniddo.dev/2021/08/how-to-secure-windows-rpc-server-and.html by @tiraniddo to understand better)
- Turn off EFS Service
- Set EFS Service Startup Type to Disabled
- Apply RPC Filter

- Certificate Mitigation: https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/07/microsoft-provides-more-mitigation-instructions-for-the-petitpotam-attack/
- Disable NTLM Authentication
- Enable SMB signing
- MSFT Suggestions: https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

RPC Filter Example:

```
rpc
filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=c681d488-d850-11d0-8c52-00c04fd90
add condition field=auth_type matchtype=equal data=16
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=c681d488-d850-11d0-8c52-00c04fd90
add filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=df1941c5-fe89-4e79-bf10-463657acf4
add condition field=auth_type matchtype=equal data=16
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=df1941c5-fe89-4e79-bf10-463657acf4
add filter
quit
```

- This filter will only allow connections through `681d488-d850-11d0-8c52-00c04fd90f7e` & `df1941c5-fe89-4e79-bf10-463657acf44d` if the authentication type is `Kerberos (16)` and the authentication type is `RPC_C_AUTHN_LEVEL_PKT_PRIVACY (6)`. This is going to prevent NTLM from being used and inturn relay from being performed.

- Due to `RPC_C_AUTHN_LEVEL_PKT_PRIVACY (6)` being set, this will also block [CVE-2021-43893](CVE-2021-43893) as well.

- Another option is a filter James Forshaw created: https://gist.github.com/tyranid/5527f5559041023714d67414271ca742

Notes:

- Findings were made surrounding the domain joined compromise version of this attack, not the local privilege escalation implementation.

Useful Resources:

- Technique References:
  - https://gist.github.com/tyranid/5527f5559041023714d67414271ca742
  - https://www.bleepingcomputer.com/news/microsoft/windows-security-update-blocks-petitpotam-ntlm-relay-attacks/
  - https://bugs.chromium.org/p/project-zero/issues/detail?id=2228
  - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43893
- Mitigation References: https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429"