Security Advisory: MSRPC Printer Spooler Relay (CVE-2021-1678)

January 22, 2021 | Eyal Karni and Alex Ionescu | Exposure Management • Identity Protection

On Patch Tuesday, January 12, 2021, Microsoft released a patch for CVE-2021-1678, an important vulnerability discovered by CrowdStrike® researchers. This vulnerability allows an attacker to relay NTLM authentication sessions to an attacked machine, and use a printer spooler MSRPC interface to remotely execute code on the attacked machine. A similar MSRPC relay first appeared in "Relaying NTLM authentication over RPC" by Sylvain Heiniger from Compass Security. In his blog, Sylvain describes how he was able to take advantage of an insecure authentication level on an MSRPC interface to achieve remote code execution via NTLM relay.

In this blog post, we show how to take advantage of the IRemoteWinSpool MSRPC interface, and how companies can protect themselves from this vulnerability. The exploitation technique resembles other previous printer spooler vulnerability exploitations such as PrintDemon: Print Spooler Privilege Escalation, Persistence and Stealth (CVE-2020-1048 and more). **Here are the technical details:**

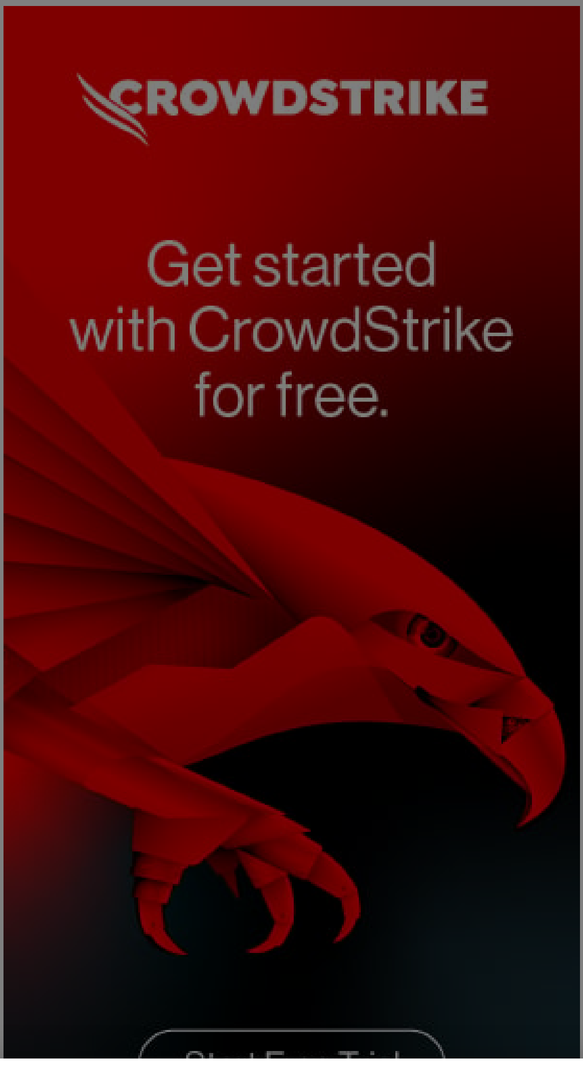
NTLM Relay Basics

The NTLM authentication protocol is susceptible to relay attacks. NTLM relay is a common attack technique where an attacker that compromises one machine can move laterally to other machines by using NTLM authentications

CATEGORIES

Cloud & Application Security	104
Counter Adversary Operations	184
Endpoint Security & XDR	307
Engineering & Tech	78
Executive Viewpoint	162
Exposure Management	84
From The Front Lines	190
Identity Protection	37
Next-Gen SIEM & Log Management	91
Public Sector	37
Small Business	8

CONNECT WITH US



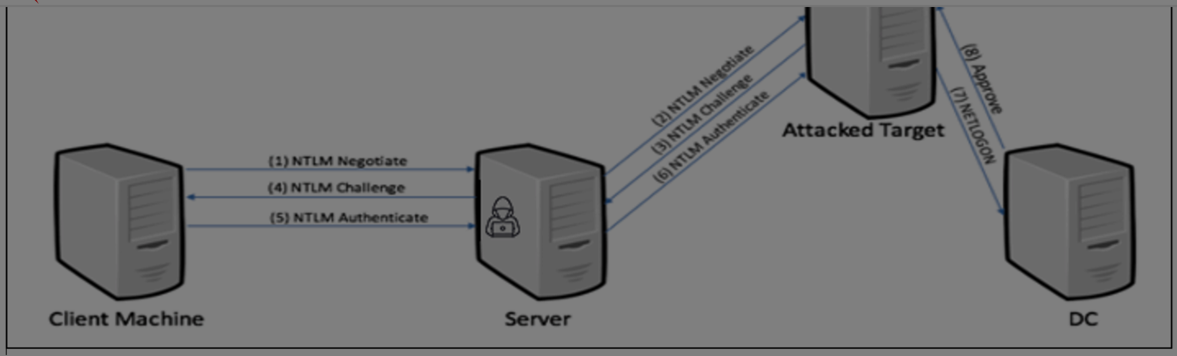


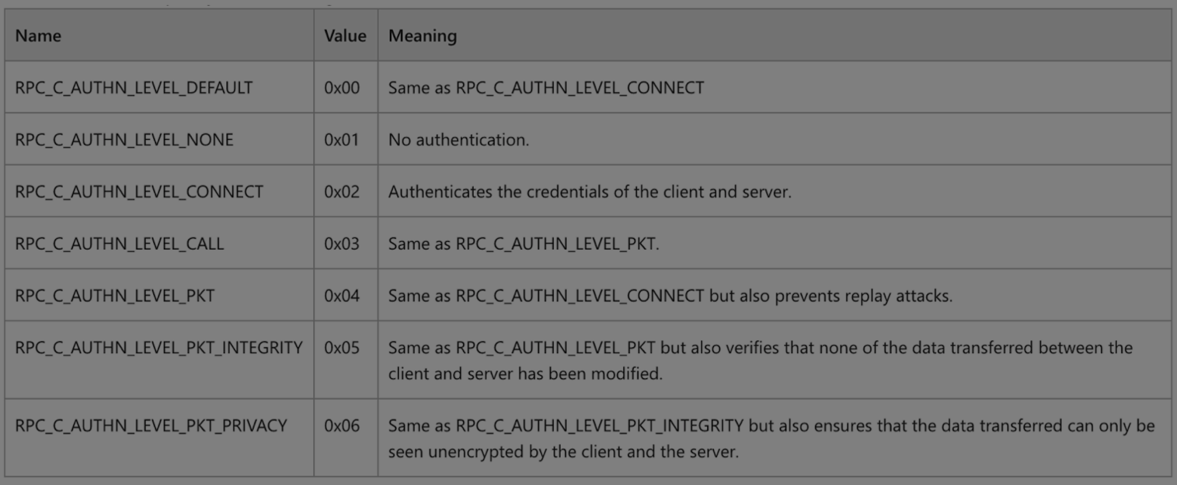
Figure 1. NTLM relay basic flow

Over the years, Microsoft has developed several mitigations for thwarting NTLM relay attacks. You can find a more detailed introduction to NTLM relay in a previously published CrowdStrike blog.

DCE/RPC Relay

NTLM authentications can be successfully relayed from any protocol to any protocol as long as the required protections are not in place. Previous NTLM relay attacks have included targeting other protocols such as Server Message Block (SMB) and LDAP/S. In this blog, we focus on targeting MSRPC. For SMB and LDAP, the main protection from NTLM relay is packet signing, which is enforced using GPO ("Microsoft network server: Digitally sign communications (always)" (Windows 10) — Windows security).

MSRPC enforces relay and man-in-the-middle (MITM) packet security differently. MSRPC servers define the level of authentication they require. This level determines the features that the underlying authentication mechanism must provide for authenticating to this server (interface):



Name	Value	Meaning
RPC_C_AUTHN_LEVEL_DEFAULT	0x00	Same as RPC_C_AUTHN_LEVEL_CONNECT
RPC_C_AUTHN_LEVEL_NONE	0x01	No authentication.
RPC_C_AUTHN_LEVEL_CONNECT	0x02	Authenticates the credentials of the client and server.
RPC_C_AUTHN_LEVEL_CALL	0x03	Same as RPC_C_AUTHN_LEVEL_PKT.
RPC_C_AUTHN_LEVEL_PKT	0x04	Same as RPC_C_AUTHN_LEVEL_CONNECT but also prevents replay attacks.
RPC_C_AUTHN_LEVEL_PKT_INTEGRITY	0x05	Same as RPC_C_AUTHN_LEVEL_PKT but also verifies that none of the data transferred between the client and server has been modified.
RPC_C_AUTHN_LEVEL_PKT_PRIVACY	0x06	Same as RPC_C_AUTHN_LEVEL_PKT_INTEGRITY but also ensures that the data transferred can only be seen unencrypted by the client and the server.

Figure 2. MSRPC authentication levels

An authentication level of RPC_C_AUTHN_LEVEL_CONNECT authenticates the user on the initial request (the bind request) but doesn't enforce any encryption or signing on the commands transferred. An interface that allows this authentication level makes itself vulnerable to NTLM relay attack. Because of this inherent weakness, one would expect the MSRPC API for server registration to implicitly choose the secured option by default and reject clients having an authentication level less than above, the task scheduler interface was exploited.

Print Spooler Privilege Escalation

While looking for vulnerable RPC interfaces that don't require any form of packet security, we found an interesting vulnerable interface: IRemoteWinspool, an RPC interface for remote printer spooler management. Working on this research, we recalled a prior one: PrintDemon: Print Spooler Privilege Escalation, Persistence and Stealth (CVE-2020-1048 and more) by Alex Ionescu and Yarden Shafir. In the blog, they show how the printer spooler interface could have been exploited to write arbitrary files as SYSTEM even when the initiating user didn't have sufficient permissions to perform such file operations. Our case, however, is different. Since we used NTLM relay, the exploitation involved using an NTLM session from a sufficiently privileged user account to execute a sequence of RPC operations that yield the desired effect. Piecing all of this together for a working exploit yields the following sequence:

1. An NTLM session is established with the relay machine controlled by the attacker.
2. The attacker binds to the IRemoteWinspool interface on a desired target and chooses the authentication level of RPC_C_AUTHN_LEVEL_CONNECT.
3. The NTLM authentication is relayed by the attacker over the established RPC channel.

4. A series of RPC commands similar to the PrinterDemon exploit flow is executed:

    - RpcAsyncInstallPrinterDriverFromPackage (Opnum 62) — Installing "Generic/Text" printer driver
    - RpcAsyncOpenPrinter (Opnum 0)
    - RpcAsyncXcvData (Opnum 33) — Add port
    - RpcAsyncAddPrinter (Opnum 1) — Add a printer with the mentioned driver
    - RpcAsyncStartDocPrinter(Opnum 10) — Start a new document
    - RpcAsyncWritePrinter (Opnum 12) — Write to new document

We have implemented a working proof of concept (POC) of the attack that will be released soon. Our code is based on impacket with the MSRPC relay implementation by Compass Security (replacing TSCH interface with IRemoteWinspool) and our implementation of the print spooler escalation flow.

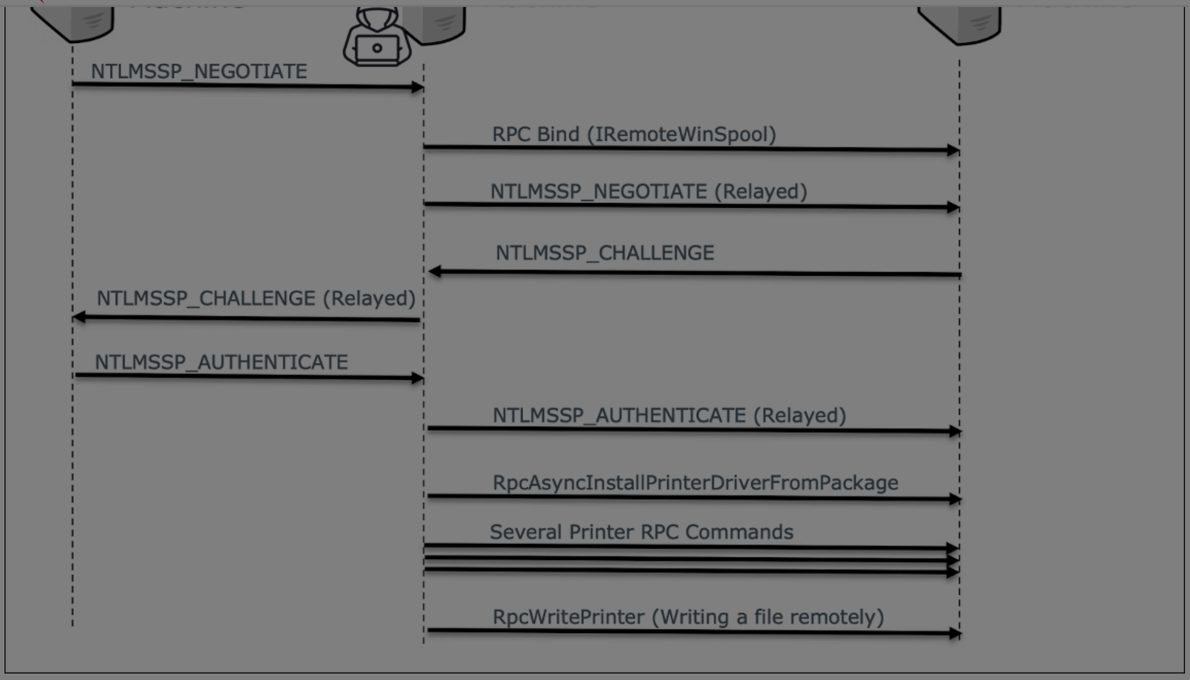
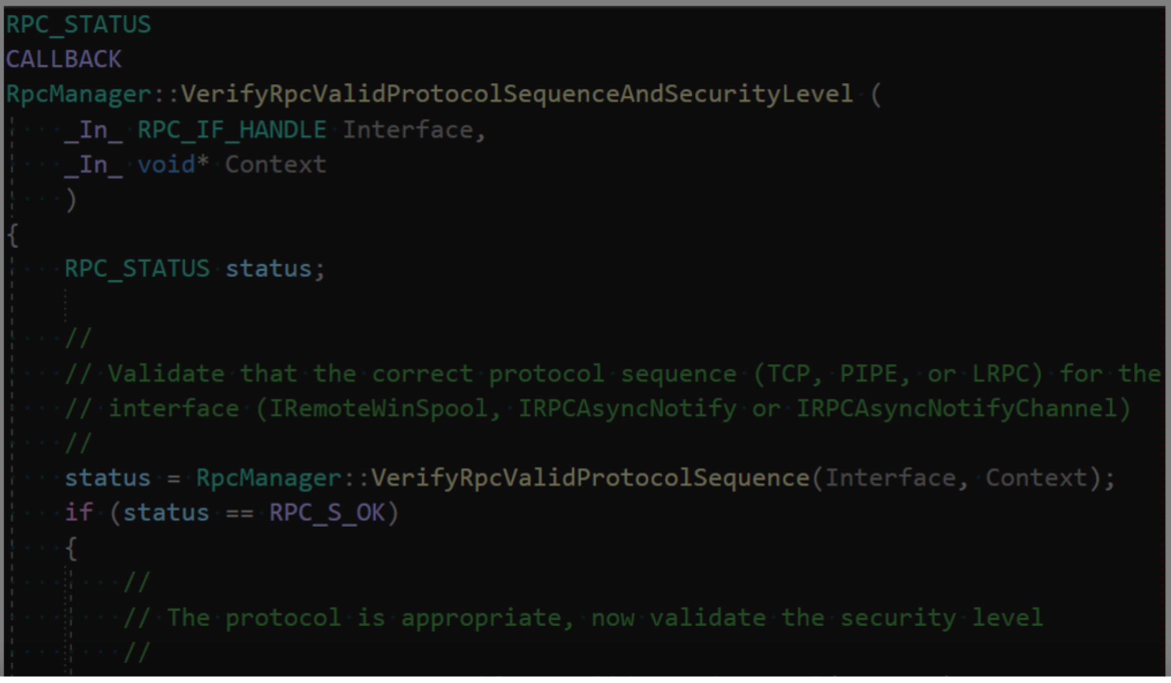

NTLMSSP_NEGOTIATE
RPC Bind (IRemoteWinSpool)
NTLMSSP_NEGOTIATE (Relayed)
NTLMSSP_CHALLENGE
NTLMSSP_CHALLENGE (Relayed)
NTLMSSP_AUTHENTICATE
NTLMSSP_AUTHENTICATE (Relayed)
RpcAsyncInstallPrinterDriverFromPackage
Several Printer RPC Commands
RpcWritePrinter (Writing a file remotely)

Figure 3. CVE-2021-1678 exploitation flow

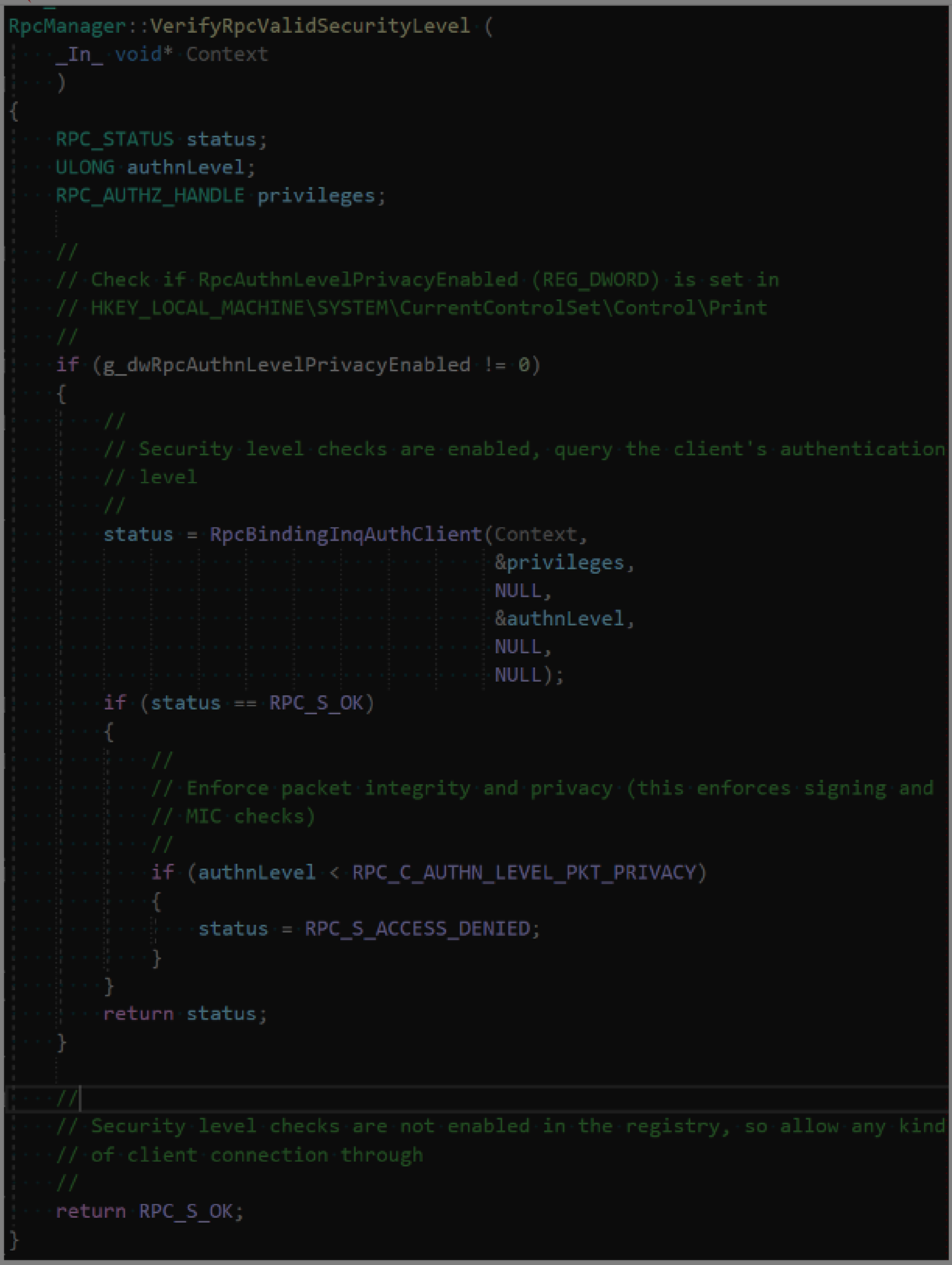
Fix Analysis

When patching the original issue identified by Sylvain Heiniger, Microsoft added the appropriate checks in the IfCallback used by the Task Scheduler service, without any larger change to the RPC runtime, perhaps because of compatibility issues. With our submission of a second instance of the same class of issue, we did not know whether Microsoft would attempt another targeted fix or a larger change. We reverse-engineered the implementation of IRemoteWinspool, which is located in Spoolsv.exe, and we found that a shared function, called RpcManager::VerifyRpcValidProtocolSequence, is used for a few of the different RPC interfaces, including IRemoteWinSpool. Originally, this function validated if the ncacn_ip_tcp protocol sequence was being used for IRemoteWinspool, which ensures that only remote TCP/IP clients are accepted (and not SMB pipe and/or local ALPC clients). As expected, no checks were done for the authentication security level. After the patch, a new IfCallback function is added into the binary instead, which we show the pseudo-code for below:



```
RPC_STATUS
CALLBACK
RpcManager::VerifyRpcValidProtocolSequenceAndSecurityLevel (
    _In_ RPC_IF_HANDLE Interface,
    _In_ void* Context
    )
{
    RPC_STATUS status;

    //
    // Validate that the correct protocol sequence (TCP, PIPE, or LRPC) for the
    // interface (IRemoteWinSpool, IRPCAsyncNotify or IRPCAsyncNotifyChannel)
    //
    status = RpcManager::VerifyRpcValidProtocolSequence(Interface, Context);
    if (status == RPC_S_OK)
    {
        //
        // The protocol is appropriate, now validate the security level
        //
```



```
RpcManager::VerifyRpcValidSecurityLevel (
    _In_ void* Context
    )
{
    RPC_STATUS status;
    ULONG authnLevel;
    RPC_AUTHZ_HANDLE privileges;

    //
    // Check if RpcAuthnLevelPrivacyEnabled (REG_DWORD) is set in
    // HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print
    //
    if (g_dwRpcAuthnLevelPrivacyEnabled != 0)
    {
        //
        // Security level checks are enabled, query the client's authentication
        // level
        //
        status = RpcBindingInqAuthClient(Context,
                                         &privileges,
                                         NULL,
                                         &authnLevel,
                                         NULL,
                                         NULL);
        if (status == RPC_S_OK)
        {
            //
            // Enforce packet integrity and privacy (this enforces signing and
            // MIC checks)
            //
            if (authnLevel < RPC_C_AUTHN_LEVEL_PKT_PRIVACY)
            {
                status = RPC_S_ACCESS_DENIED;
            }
        }
        return status;
    }

    //
    // Security level checks are not enabled in the registry, so allow any kind
    // of client connection through
    //
    return RPC_S_OK;
}
```

Figure 5. Security level validation after the patch enforcing RPC_C_AUTHN_LEVEL_PKT_PRIVACY or above

This is another tactical fix similar to the one for the ITaskScheduler interface, where the authentication level of the client is now checked against RPC_C_AUTHN_LEVEL_PKT_PRIVACY, and the call rejected with RPC_S_ACCESS_DENIED if this is not set. Interestingly, however, we noted that this code path is *only taken if a registry value is set*, which does not appear to be enabled even after applying the patch.

As shown in the code in Figure 5, the REG_DWORD value RpcAuthnLevelPrivacyEnabled must be set to 1 in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print key, or otherwise this additional check is not performed, and the system remains vulnerable to attack. Now that the patch is released, this behavior is explained by Microsoft in the following support article, which confirms that by default, RPC printer bindings will *still* allow for vulnerable connections. In June's update, a mitigate the discovered attack. Note that patching alone is not enough. Until you change the registry settings according to the Microsoft guide, you will still be vulnerable to this attack. For emergency patching situations, see this video on how Falcon Spotlight can help your organization stay secure.

2. **Configure secure NTLM settings:** Some NTLM relay mitigations are not enabled by default, leaving your network insecure. Most notable are SMB signing, LDAP signing and LDAPS channel binding. Review these security settings and make sure your network is fully protected.
3. **Track NTLM usage:** Ultimately, in the authors' opinion, the goal of any organization should be to completely stop using NTLM. This recommendation is based on various NTLM security issues we have discovered and blogged about in the past.

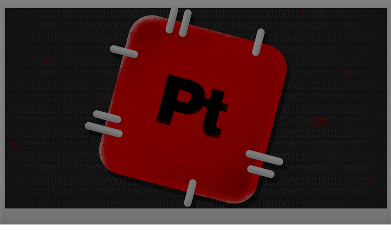
4. **Detect NTLM relay attacks:** Securing and removing NTLM in your network is a long and complex IT project. As long as your network is not fully secure, we recommend having a security product that helps detect NTLM anomalies and NTLM relay attacks.

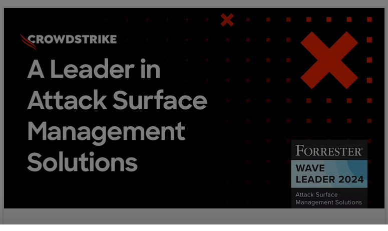
Additional Resources

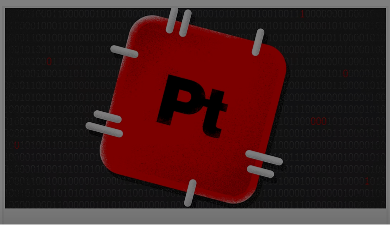
- *Learn more by reading the white paper, "The Security Risks of NTLM."*
- *Learn how Falcon Spotlight can help you discover and manage vulnerabilities within your organization.*
- *Learn about past NTLM relay vulnerabilities discovered by the team.*
- *Visit the CrowdStrike Falcon® Identity Protection solutions webpage.*
- *Request a demo of CrowdStrike Falcon Zero Trust or Falcon Identity Threat Detection products.*
- *Read expert insights and analysis on other complex threats — download the CrowdStrike 2020 Global Threat Report.*

Tweet Share

Related Content




CROWDSTRIKE
A Leader in Attack Surface Management Solutions
FORRESTER WAVE LEADER 2024



CROWDSTRIKE | BLOG

Featured Recent Video Category Start Free Trial

« Active Directory Open to More NTLM Attacks: Drop The MIC 2 (CVE 2019-1166) and Exploiting LMv2 Clients (CVE-2019-1338)

How to Stay Cyber Aware of Weaknesses and Vulnerabilities in Your Environment »