CROWDSTRIKE | BLOG

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

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 directed at the compromised server.

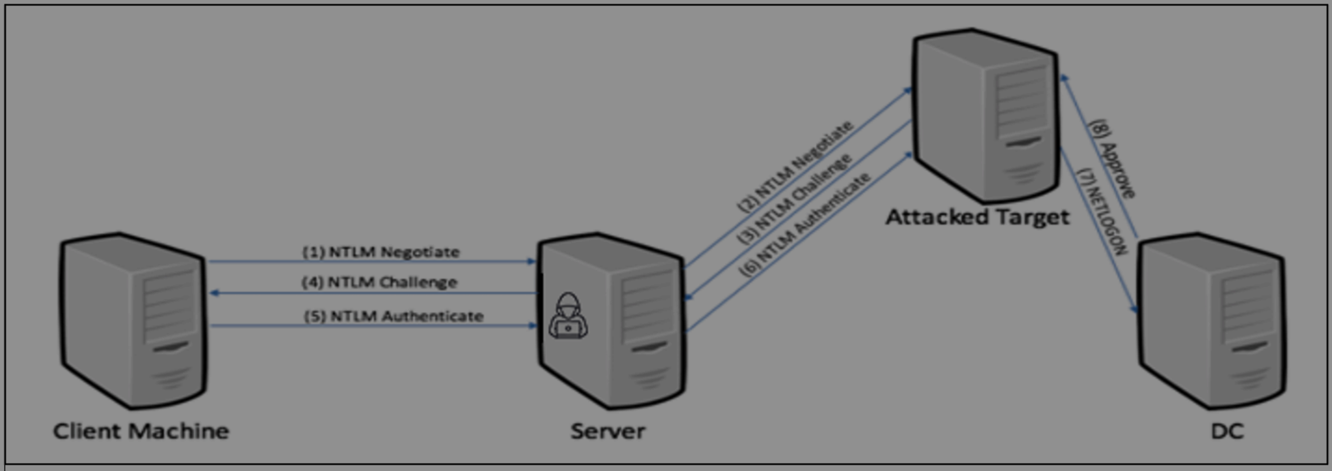
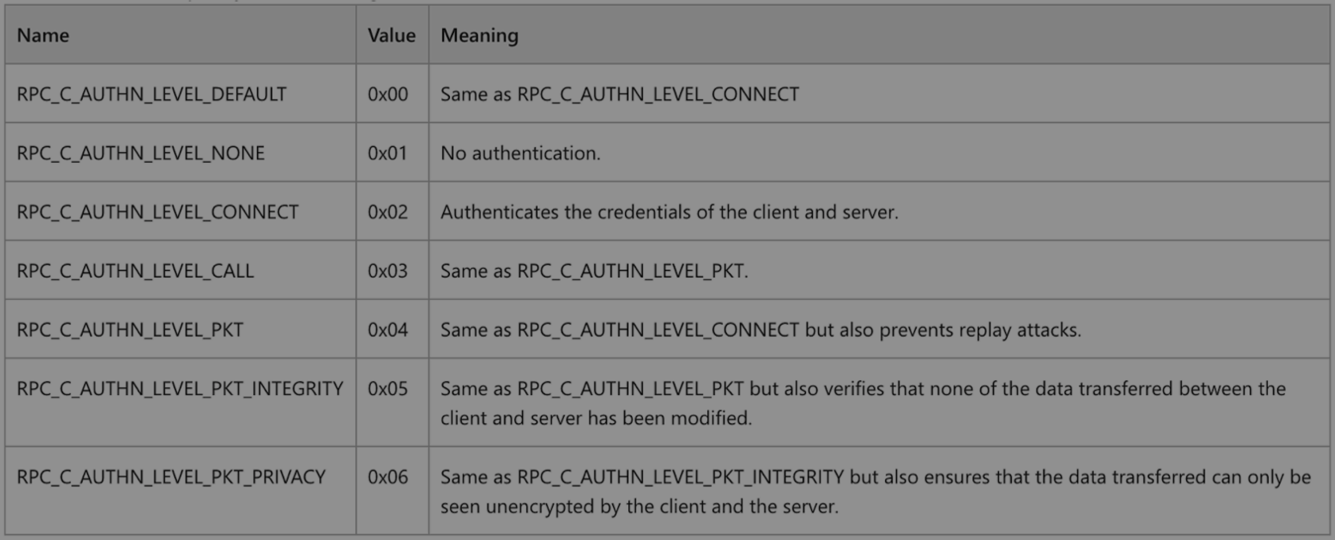


Figure 1. NTLM relay basic flow

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.

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 RPC_C_AUTHN_LEVEL_PKT_INTEGRITY. However, in the MSRPC case, it is every

Featured
Recent
Video
Category

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:

Featured
Recent
Video
Category

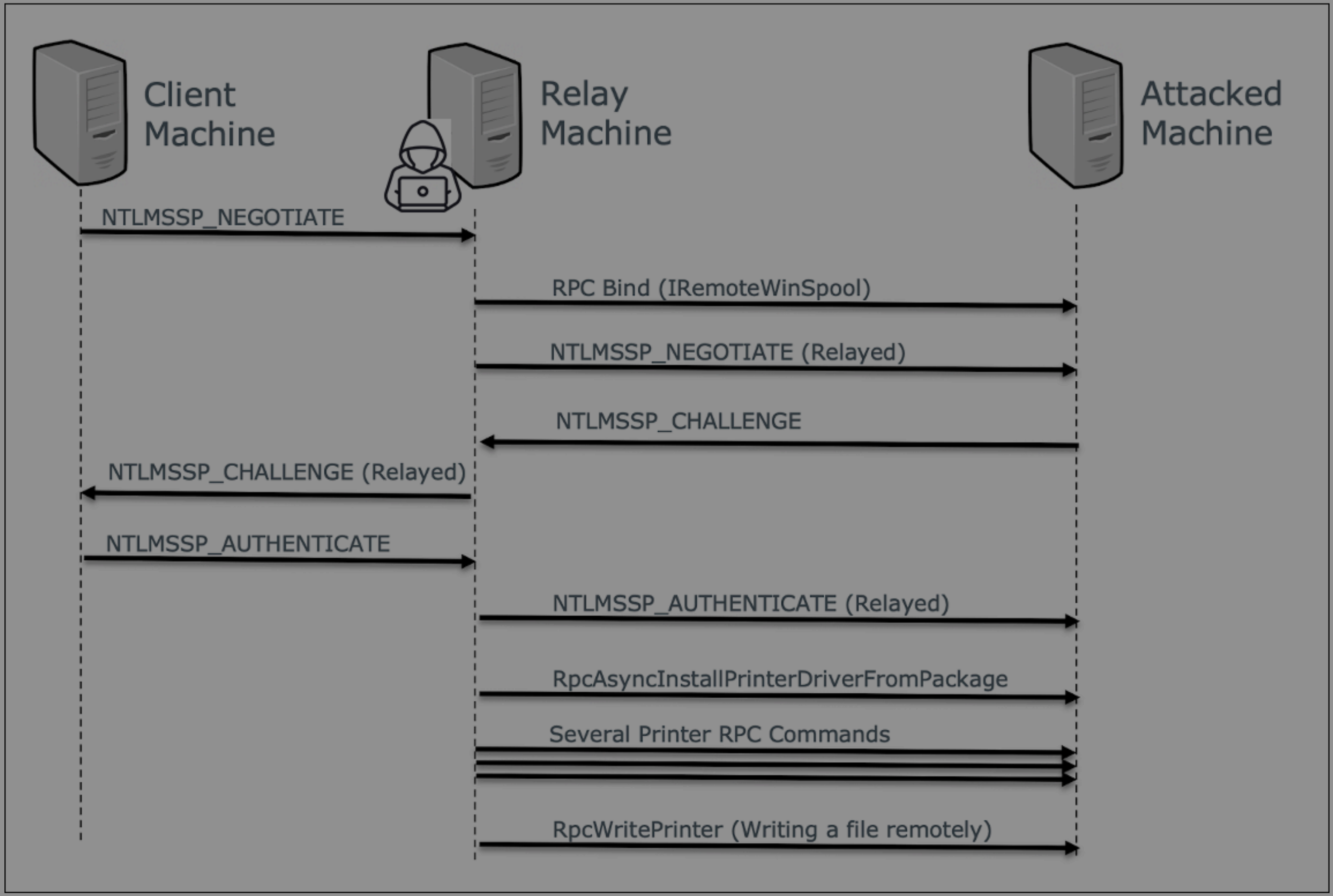
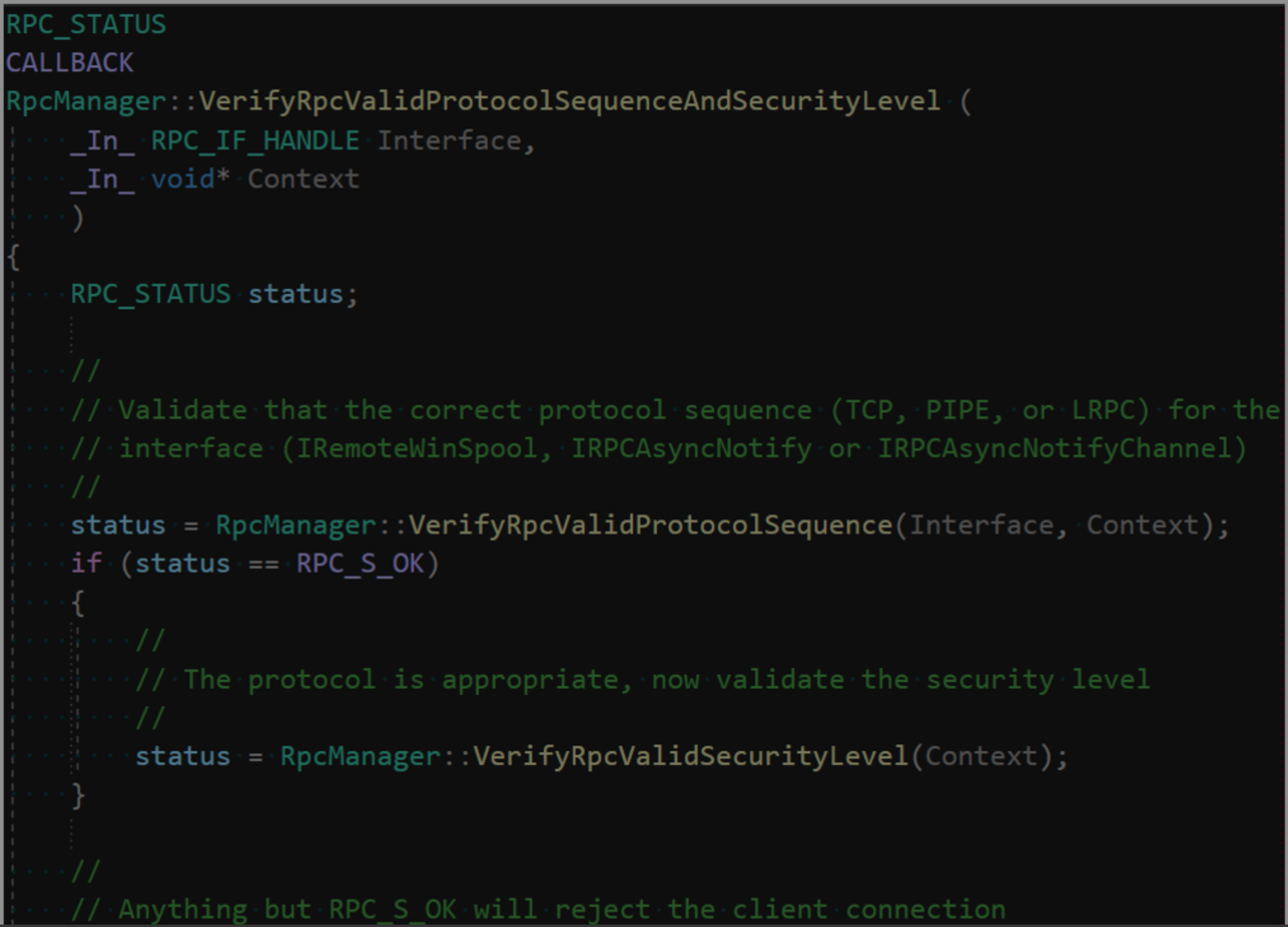

Client Machine
Relay Machine
Attacked Machine
NTLMSSP_NEGOTIATE
RPC Bind (IRemoteWinSpool)
NTLMSSP_NEGOTIATE (Relayed)
NTLMSSP_CHALLENGE
NTLMSSP_CHALLENGE (Relayed)
NTLMSSP_AUTHENTICATE
NTLMSSP_AUTHENTICATE (Relayed)
RpcAsyncInstallPrinterDriverFromPackage
Several Printer RPC Commands
RpcWritePrinter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

Figure 3. CVE-2021-1678 exploitation flow

level. After the patch, a new IfCallback function is added into the binary instead, which we show the pseudo-code for below:



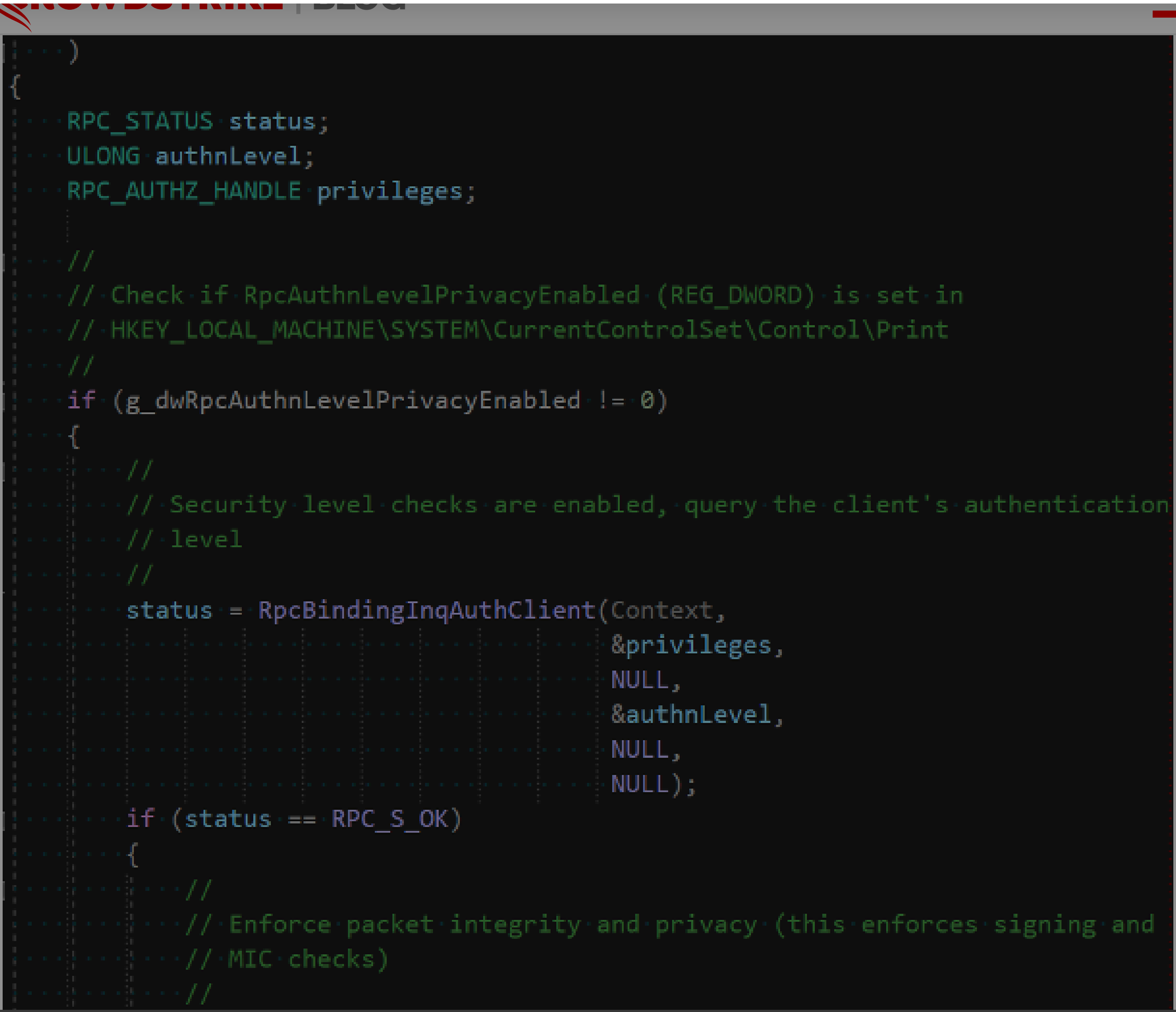
```
RPC_STATUS
CALLBACK
RpcManager::VerifyRpcValidProtocolSequenceAndSecurityLevel (
    _In_ RPC_IF_HANDLE Interface,
    _In_ void* Context
    )
{
    RPC_STATUS status;

    //
    // 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
        //
        status = RpcManager::VerifyRpcValidSecurityLevel(Context);
    }

    //
    // Anything but RPC_S_OK will reject the client connection
```

Featured
Recent
Video
Category

Featured
Recent
Video
Category



```
    )
{
    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)
            //
```

Featured
Recent
Video
Category

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 second patch will be released, making secure registry settings the default.

How Can I Protect My Network?

We suggest taking a few steps to protect your network from this vulnerability and other similar NTLM relay attacks:

Featured
Recent
Video
Category

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.*

X Tweet in Share

October 2024 Patch Tuesday: Two Zero-Days and Three Critical Vulnerabilities Amid 118 CVEs

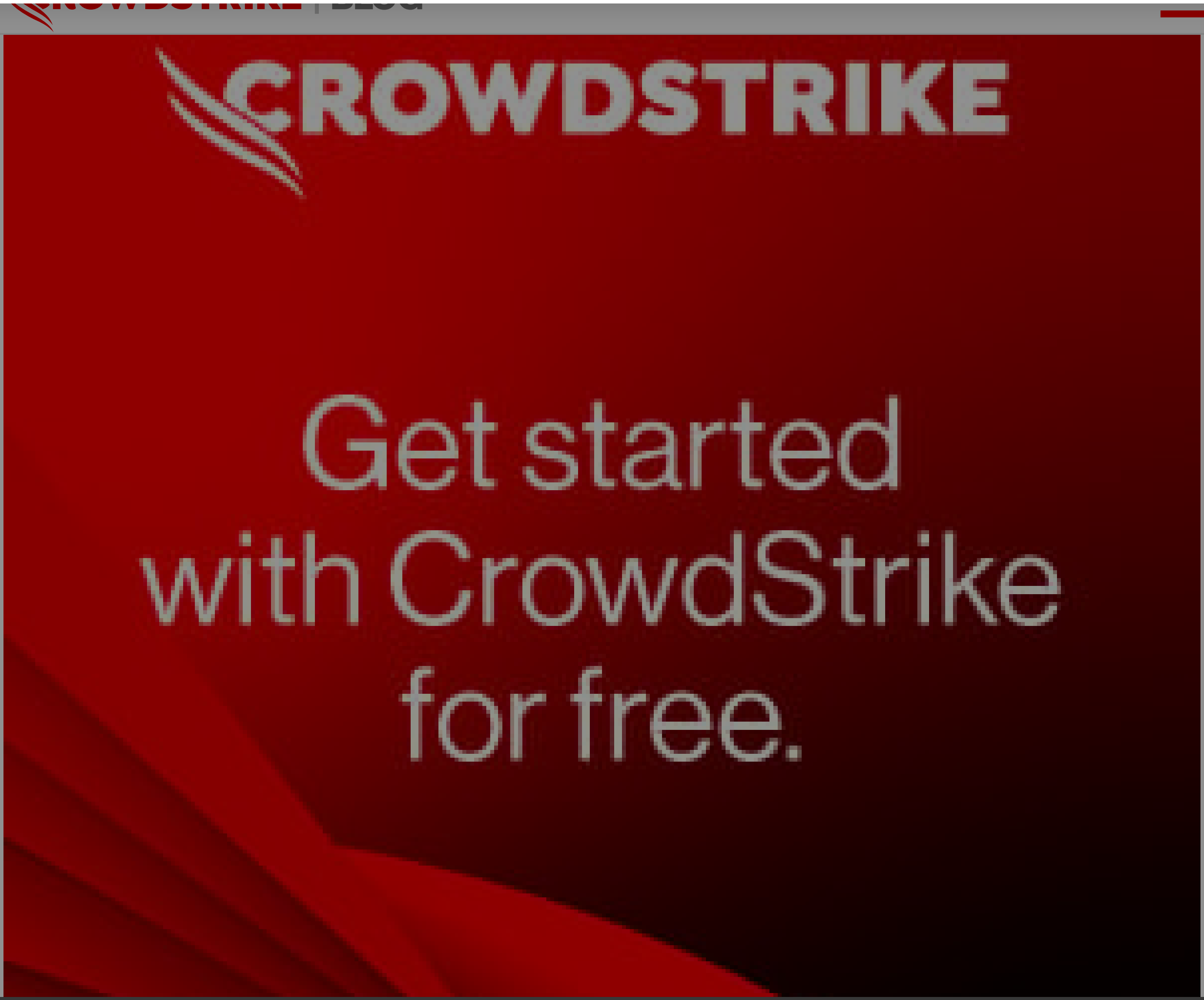
CrowdStrike Named a Leader in the 2024 Forrester Wave™: Attack Surface Management Solutions

September 2024 Patch Tuesday: Four Zero-Days and Seven Critical Vulnerabilities Amid 79 CVEs

CATEGORIES

Cloud & Application Security	104
Counter Adversary Operations	184
Endpoint Security & XDR	306
Engineering & Tech	78
Executive Viewpoint	162
Exposure Management	84
From The Front Lines	190
Identity Protection	37

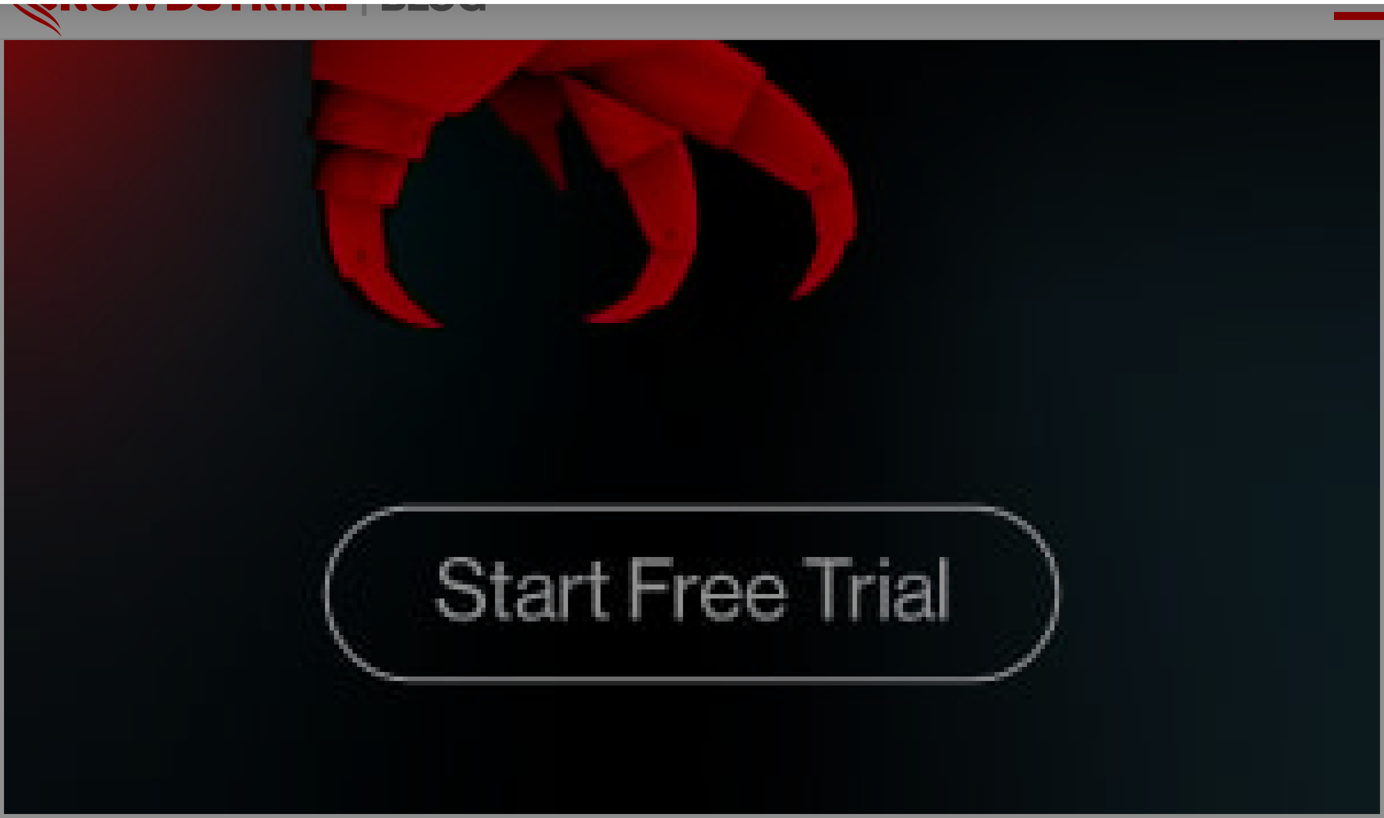
Featured
Recent
Video
Category



Featured

Recent

Video


Start Free Trial

Recognizing the Resilience of the CrowdStrike Community

September 25, 2024

CrowdStrike Drives Cybersecurity Forward with New Innovations Spanning AI, Cloud, Next-Gen SIEM and Identity Protection

September 18, 2024

Featured
Recent
Video
Category