CalCom

RDS HARDENING RECOMMENDATIONS

RDS has been dominating the headlines the last few months with some of the most harmful vulnerabilities. But first of all, let's fully understand RDS, its functions, and its structure.

Remote Desktop Service (RDS) is a component of Microsoft Windows that allows users to take control of a remote computer or a virtual machine which supports the Remote Desktop Protocol (RDP) via a network connection.

RDS KEY COMPONENTS

The **Terminal Server** is the server component of Terminal Services. It handles the job of authenticating clients, as well as making applications that are accessible to the user available remotely. The Terminal Server is the key component of RDS and listens on TCP port 3389.

The **Remote Desktop Gateway** service component can tunnel the RDP session using an HTTPS channel. This increases the security of RDS by encapsulating the session with Transport Layer Security (TLS). This also allows the option of using the Internet as the RDP client.

Once a client initiates a connection and is informed of a successful invocation of the terminal services stack at the server, it loads up the device as well as the keyboard/mouse drivers.

RDP vulnerabilities emerged frequently this year, starting with Checkpoint's discovery of the Microsoft RDP clipboard vulnerability and continuing with the wormable BlueKeep vulnerability, the damage potential of which is estimated to be as severe as that of WannaCry. There's also the recently discovered DejaBlue, which resembles BlueKeep in its properties with a severity code of 9.8, affecting over 1 million machines, but it might be even easier to exploit.

RDP CLIPBOARD VULNERABILITY

Microsoft's clipboard sharing channel supports several data formats, such as CF_HDROP, which is responsible for the "Copy & Paste" feature. When used, it allows the client to simply copy a group of files from one computer to the other. If the client himself fails to prevent malicious files from entering his computer via this feature, he could be vulnerable to a path traversal attack. The server can then drop malicious files in arbitrary paths on the client's computer. In other words, the client's approval of the files is the only thing protecting him from this vulnerability. Considering the fact that the client doesn't even need to verify the received files coming from the RDP server, it is almost impossible to detect the attack.

When initiating a demo attack, the researchers killed the rdpclip.exe port at the RDP server and replaced it with their own process that enabled adding a malicious file to every "Copy & Paste" action. There's usually no need for any elevated permissions in order to perform the attack.

BLUEKEEP VULNERABILITY

The root cause of BlueKeep seems to be a Use After Free (UAF) condition which exists within the termdd.sys, which is the RDP kernel driver. It can be exploited remotely by an unauthenticated attacker by opening an RDP connection to a remote computer called a channel – in this case, a default RDP channel called MS_T210 – and sending specially crafted data to it. The result is that the program tries to use memory after it was supposed to discard it.

BlueKeep is an extremely critical problem for three main reasons:
1. There's no need for any authentication in order to execute arbitrary code and take control of the targeted computer. Any remote attacker can attack your computer just by sending specially crafted requests to the device's RDS via the RDP with zero interaction with the user.
2. An attacker can execute any arbitrary code once the targeted system is under his control.
3. Being a 'wormable' vulnerability, once a computer gets infected, the entire network can get infected really fast.

DEJABLUE VULNERABILITY

DejaBlue is actually a group of 4 RDP vulnerabilities: CVE-2019-1181, CVE-2019-1182, CVE-2019-1222 & CVE-2019-1226. All four CVEs were given a critical severity code of 9.8 and are believed to have affected somewhere around 1 million machines.

The DejaBlue vulnerabilities are in the early stages of the RDP connection. The flaws precede the authentication phase, thus there is no need for passwords of keys to breach the system, which eventually can lead to remote code execution.

In addition, CVE-2019-1181 and CVE-2019-1182 have the potential of being 'wormable', spreading inside the network, crossing between different internal networks and moving between internal and external networks. This, of course, adds another dimension of severity to DejaBlue.

All in all, it is pretty clear now that what used to be estimated as a secure service and protocol is now revealing its ugly truth. This situation requires IT ops and security teams to change their approach and put more effort into RDS configuration hardening.

The most straightforward action that needs to be done is to disable the service in any machine that doesn't require it for its functionality. Might sounds easy, but mapping those machines is very painful and labor-demanding to even understand which machine won't break when you disable the protocol.

When it comes to machines that must have RDS enabled for functionality, it is important to understand the most secure way to configure it.

As hardening is CalCom's specialty, our team of experts conducted a list of values that need to be configured at a certain value in order to make sure that the RDS is as secure as it can be. Here is a list of those values and their recommended state:

REQUIRE USER AUTHENTICATION FOR REMOTE CONNECTIONS BY USING NETWORK LEVEL AUTHENTICATION- ENABLE

POLICY DESCRIPTION

This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase "Network Level Authentication supported". If you disable or do not configure this policy setting, Network Level Authentication is not required for user authentication before allowing remote connections to the RD Session Host server. You can specify that Network Level Authentication be required for user authentication by using Remote Desktop Session Host Configuration tool or the Remote tab in System Properties.

POTENTIAL VULNERABILITY

By not configuring this value to Enable, you are expose to the BlueKeep vulnerability and any remote attacker will be able to attack your computer (see above).

DO NOT ALLOW CLIENT PRINTER REDIRECTION- ENABLED

POLICY DESCRIPTION

This policy setting allows you to specify whether to prevent the mapping of client printers in Remote Desktop Services sessions. You can use this policy setting to prevent users from redirecting print jobs from the remote computer to a printer attached to their local (client) computer. By default, Remote Desktop Services allows this client printer mapping. If you enable this policy setting, users cannot redirect print jobs from the remote computer to a local client printer in Remote Desktop Services sessions. If you disable this policy setting, users can redirect print jobs with client printer mapping. If you do not configure this policy setting, client printer mapping is not specified at the Group Policy level. However, an administrator can still disable client printer mapping by using the Remote Desktop Session Host Configuration tool.

POTENTIAL VULNERABILITY

printers installed in company networks have no security by default. Worst case is that most printers provide full administrative access until the network administrator reconfigures the network once in a while. This results in serious threats and misuse of data, creating a platform for attacking all the systems connected to the network. Therefore, unsecured multi-functional printers which can be accessed by a remote user create a threat that can be utilized by spies or hackers.

DO NOT ALLOW CLIPBOARD REDIRECTION- ENABLED

POLICY DESCRIPTION

Specifies whether to prevent the sharing of clipboard contents (clipboard redirection) between a remote computer and a client computer during a Remote Desktop Services session. You can use this setting to prevent users from redirecting clipboard data to and from the remote computer and the local computer. By default, Remote Desktop Services allows clipboard redirection. If the status is set to Enabled, users cannot redirect clipboard data. If the status is set to Disabled, Remote Desktop Services always allows clipboard redirection. If the status is set to Not Configured, clipboard redirection is not specified at the Group Policy level. However, an administrator can still disable clipboard redirection using the Remote Desktop Session Host Configuration tool.

POTENTIAL VULNERABILITY

Microsoft's clipboard sharing channel supports several data formats such as CF_HDROP that is responsible for the "Copy & Paste" feature. When used, it allows to simply copy a group of files from one computer to the other. If the client itself fails to prevent malicious files from entering his computer via this feature, he could be vulnerable to a path traversal attack. The server can then drop malicious files in arbitrary paths on the client's computer. In other words, the client's approval of the files is the only thing protecting him from this vulnerability. Considering the fact that the client doesn't even need to verify the received files coming from the RDP server, it is almost impossible to detect the attack.

DO NOT ALLOW COM PORT REDIRECTION- ENABLED

POLICY DESCRIPTION

Specifies whether to prevent the redirection of data to client COM ports from the remote computer in a Remote Desktop Services session. You can use this setting to prevent users from redirecting data to COM port peripherals or mapping local COM ports while they are logged on to a Remote Desktop Services session. By default, Remote Desktop Services allows this COM port redirection. If the status is set to Enabled, users cannot redirect server data to the local COM port. If the status is set to Disabled, Remote Desktop Services always allows COM port redirection. If the status is set to Not Configured, COM port redirection is not specified at the Group Policy level. However, an administrator can still disable COM port redirection using the Remote Desktop Session Host Configuration tool.

POTENTIAL VULNERABILITY

When Disabled or not configured, the attacker can redirect potential harmful data to client COM ports from the remote computer or terminal server. Attacker can also map a local COM port while he is logged to the RDS session.

DO NOT ALLOW DRIVE REDIRECTION- ENABLED

POLICY DESCRIPTION

Specifies whether to prevent the mapping of client drives in a Remote Desktop Services session (drive redirection). By default, an RD Session Host server maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or Computer in the format <driveletter> on <computername>. You can use this setting to override this behavior. If the status is set to Enabled, client drive redirection is not allowed in Remote Desktop Services sessions. If the status is set to Disabled, client drive redirection is always allowed. If

the status is set to Not Configured, client drive redirection is not specified at the Group Policy level. However, an administrator can still disable client drive redirection by using the Remote Desktop Session Host Configuration tool.

POTENTIAL VULNERABILITY
Preventing users from sharing the local drives on their client computers to Remote Session Hosts that they access helps reduce possible exposure of sensitive data. Attacker can leverage this function in order to forward data from the user's Terminal Server session to the user's local computer without any direct user interaction.

DO NOT ALLOW LPT PORT REDIRECTION- ENABLED

POLICY DESCRIPTION
Specifies whether to prevent the redirection of data to client LPT ports during a Remote Desktop Services session. You can use this setting to prevent users from mapping local LPT ports and redirecting data from the remote computer to local LPT port peripherals. By default, Remote Desktop Services allows this LPT port redirection. If the status is set to Enabled, users in a Remote Desktop Services session cannot redirect server data to the local LPT port. If the status is set to Disabled, LPT port redirection is always allowed. If the status is set to Not Configured, LPT port redirection is not specified at the Group Policy level. However, an administrator can still disable local LPT port redirection using the Remote Desktop Session Host Configuration tool.

POTENTIAL VULNERABILITY
If value is configured to Disabled or Not Configured, attacker can leverage it to map the client's LPT ports. In addition, he can use the port to redirect data from the Terminal Server to the local LTP ports.

DO NOT ALLOW PASSWORDS TO BE SAVED- ENABLED

POLICY DESCRITION
Controls whether passwords can be saved on this computer from Remote Desktop Connection. If you enable this setting the password saving checkbox in Remote Desktop Connection will be disabled and users will no longer be able to save passwords. When a user opens an RDP file using Remote Desktop Connection and saves his settings, any password that previously existed in the RDP file will be deleted. If you disable this setting or leave it not configured, the user will be able to save passwords using Remote Desktop Connection.

POTENTIAL VULNERABILITY
Saving passwords in the Remote Desktop Client could allow an unauthorized user to establish a remote desktop session to another system.
This can be a security hazard, especially if you share the computer you are using to log onto the remote computer.

DO NOT ALLOW SUPPORTED PLUG AND PLAY DEVICE REDIRECTION- ENABLED

POLICY DESCRIPTION
This policy setting allows you to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Remote Desktop Services session. By default, Remote Desktop

Services allows redirection of supported Plug and Play devices. Users can use the “More” option on the Local Resources tab of Remote Desktop Connection to choose the supported Plug and Play devices to redirect to the remote computer. If you enable this policy setting, users cannot redirect their supported Plug and Play devices to the remote computer. If you disable this policy setting or do not configure this policy setting, users can redirect their supported Plug and Play devices to the remote computer. Note: You can also disallow redirection of supported Plug and Play devices on the Client Settings tab in the Remote Desktop Session Host Configuration tool. You can disallow redirection of specific types of supported Plug and Play devices by using the “Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions” policy settings.

POTENTIAL VULNERABILITY

RemoteFX USB device redirection goal is to enable the user to use any device he wants. But, leaving Plug and Play device redirection enabled or unconfigured can be leveraged for RemoteFX redirection attacks, in which a rogue USB can harm an RDP server. In order to mitigate unwanted RemotetFX USB redirection, ‘Do not allow supported Plug and Play device redirection’ in the RDP needs to be configured to enable.

- Set time limit for disconnected sessions- 5 minutes
- Set time limit for active but idle Remote Desktop Services sessions- 24 hours

HARDENING YOUR RDS WITHOUT BREAKING PRODUCTION – AUTOMATING THE HARDENING PROCESS

Every change in configuration can potentially damage production; therefore, every change needs to be first checked in a lab environment to understand the change’s outcomes. The length of time between establishing the policy and implementing it is often long and painful because it is usually done manually.

The CalCom Hardening Solution (CHS) will automate the entire hardening process. CHS has the unique ability to learn your production environment and determine what the impact of any change in configuration. It eliminates the need for testing in a lab environment before implementing the policy. CHS allows you to control the entire hardening process from a single user, therefore eliminating the possibility of configuration drifts. Our product will continuously keep you compliant, suitable for changes in your system or in your policies.