RDP Security Explained

By Darren Fitzpatrick, John Fokker and Eamonn Ryan on Jun 24, 2019

RDP on the Radar

Recently, McAfee released a blog related to the wormable RDP vulnerability referred to as CVE-2019-0708 or "Bluekeep." The blog highlights a particular vulnerability in RDP which was deemed critical by Microsoft due to the fact that it exploitable over a network connection without authentication. These attributes make it particularly 'wormable' – it can easily be coded to spread itself by reaching out to other accessible networked hosts, similar to the famous EternalBlue exploit of 2017. This seems particularly relevant when (at the time of writing) 3,865,098 instances of port 3389 are showing as open on Shodan.

Prior to this, RDP was already on our radar. Last July, McAfee ATR did a deep dive on Remote Desktop Protocol (RDP) marketplaces and described the sheer ease with which cybercriminals can obtain access to a large variety of computer systems, some of which are very sensitive. One of the methods of RDP misuse that we discussed was how it could aid deploying a targeted ransomware campaign. At that time one of the most prolific targeted ransomware groups was SamSam. To gain an initial foothold on its victims' networks, SamSam would often rely on weakly protected RDP access. From its RDP launchpad, it would proceed to move laterally through a victim's network, successfully exploiting and discovering additional weaknesses, for instance in a company's Active Directory (AD).

In November 2018, the FBI and the Justice department indicted two Iranian men for developing and spreading the SamSam ransomware extorting hospitals, municipalities and public institutions, causing over $30 million in losses. Unfortunately, this did not stop other cybercriminals from using similar tactics, techniques and procedures (TTPs).

The sheer number of vulnerable systems in the wild make it a "target" rich environment for cybercriminals.

In the beginning of 2019 we dedicated several blogs to the Ryuk ransomware family that has been using RDP as an initial entry vector. Even though RDP misuse has been around for many years, it does seem to have gained an increased popularity amongst criminals focused on targeted ransomware.

Recent statistics showed that RDP is the most dominant attack vector, being used in 63.5% of disclosed targeted ransomware campaigns in Q1 of 2019.

Source: Coveware Q1 statistics

Securing RDP

Given the dire circumstances highlighted above it is wise to question if externally accessible RDP is an absolute necessity for any organization. It is also wise to consider how to better secure RDP if you are absolutely reliant on it. The good news is there are several easy steps that help an organization to better secure RDP access.

That is why, in this blog, we will use the adversarial knowledge from the McAfee ATR red team to explain what easy measures can be undertaken to harden RDP access.

Recommendations are additional to standard systems hygiene which should be carried out for all systems (although it becomes more important for Internet connected hosts), such as keeping all software up-to-date, and we intentionally avoid 'security through obscurity' items such as changing the RDP port number.

Do not allow RDP connections over the open Internet

To be very clear… RDP should never be open to the Internet. The internet is continuously being scanned for open port 3389 (the default RDP port). Even with a complex password policy and multi-factor authentication you can be vulnerable to denial of service and user account lockout. A much safer alternative is to use a Virtual Private Network (VPN). A VPN will allow a remote user to securely access their corporate network without exposing their computer to the entire Internet. The connection is mutually encrypted, providing authentication for both client and server, preferably using a dual factor, while creating a secure tunnel to the corporate network. As you only have access to the network you will still need to RDP to the computer but can do so more securely without exposing it to the internet.

Use Complex Passwords

An often-used alternative acronym for RDP is "Really Dumb Passwords." That short phrase encapsulates the number one vulnerability of RDP systems, simply by scanning the internet for systems that accept RDP connections and launching a brute-force attack with popular tools such as, ForcerX, NLBrute, Hydra or RDP Forcer to gain access.

Using complex passwords will make brute-force RDP attacks harder to succeed.

Below are the top 15 passwords used on vulnerable RDP systems. We built this list based on information on weak passwords shared by a friendly Law Enforcement Agency from taken down RDP shops. What is most shocking is the fact that there is such a large number of vulnerable RDP systems did not even have a password.

The TOP 15 used passwords on vulnerable RDP systems

[no password]
123456
P@ssw0rd
123
Password1
1234
password
1
12345
Password123
admin
test
test123
Welcome1
scan

Use Multi-Factor Authentication

In addition to a complex password, it is best practice use multi-factor authentication. Even with great care and diligence, a username and password can still be compromised. If legitimate credentials have been compromised, multi-factor authentication adds an additional layer of protection by requiring the user to provide a security token, e.g. a code received by notification or a biometric verification. Better yet, a FIDO based authentication device can provide an extra factor which is not vulnerable to spoofing attacks, in a similar fashion to other one-time-password (OTP) mechanisms. This increases the difficulty for an unauthorized person to gain access to the computing device.

Use an RDP Gateway

Recent versions of Windows Server provide an RDP gateway server. This provides one external interface to many internal RDP endpoints, thus simplifying management, including many of the items outlined in the following recommendations. These comprise of logging, TLS certificates, authentication to the end device without actually exposing it to the Internet, authorization to internal host and user restrictions, etc.

Microsoft provides detailed instructions for configuration of remote desktop gateway server, for Windows Server 2008 R2 as an example, over here.

Lock out users and block or timeout IPs that have too many failed logon attempts

A high number of failed logon attempts is a strong indication of a brute force attack. Limiting the number of logon attempts per user can prevent such attacks. A failed logon attempt is logged under Windows Event ID 4625. An RDP logon falls under logon type 10, RemoteInteractive. The account lockout threshold can be specified in the local group policy under security settings: Account Policies.

For logging purposes, it is best to log both failed and successful logons. Additionally, it is important to note that “specific security layer for RDP connections” needs to be enabled. Otherwise, you will be unable to tell that the logon attempt came over RDP or see the source IP address. A comparison is shown below.

Event log network logon (type 3) note no source network address

Event log RDP logon (type 10) note the source network address present

Use a Firewall to restrict access

Firewall rules can be created to restrict Remote Desktop access so that only a specific IP address or a range of IP addresses can access a given device. This can be achieved by simply opening “Windows Firewall with Advanced Security,” clicking on Inbound Rules and scrolling down to the RDP rule. A screen shot can be seen below.

Firewall settings for inbound RDP connections

Enable Restricted Admin Mode

When connecting to a remote machine via RDP, credentials are stored on that machine and may be retrievable by other users of the systems (e.g. malicious attackers). Microsoft has added restricted admin mode which instructs the RDP server not to store credentials of users who log in. Behind the scenes, the server now uses ‘network’ login rather than ‘interactive’ and therefore uses hashes or Kerberos tickets rather than passwords for authentication. Assessment of the pros and cons of this option are recommended before enabling in your environment. On the negative side, the use of network login exposes the possibility of credential reuse (pass the hash) attacks against the RDP server. Pass the hash is likely possible anyway, internally, via other exposed ports so may not significantly increase exposure there, but when including this option to Internet servers, where other ports are likely (and should be!) restricted, pass the hash is then extended to the Internet. Given the pros and cons, avoiding internal

escalation of privilege is often prioritized and therefore restricted admin mode is enabled.

Microsoft TechNet describes configuration and usage of restricted mode here.

Encryption

There are four levels of encryption supported by standard RDP: Low, Client Compatible, High, and FIPS Compliant. This is configured on the Remote Desktop server. This can be further improved upon by using Enhanced RDP Security. When Enhanced RDP security is used, encryption and server authentication are implemented by external security protocols, e.g. TLS or CredSSP. One of the key benefits of Enhanced RDP Security is that it enables the use of Network Level Authentication (NLA) when using CredSSP as the external security protocol.

Certificate management is always a complexity, but Microsoft does provide this through the use of Active Directory Certificate Services (ADCS). Certificates can be pushed using Group Policy Objects (GPO) where this is available. Incompatible operating system environments must import certificates via the web interface exposed at https://<server>/Certsrv.

Enable Network Level Authentication (NLA)

To reduce the amount of initially required server resources, and thereby mitigate against denial of service attacks, network level authentication (NLA) can be used. Within this mode, strong authentication takes place before the remote desktop connection is established, using the Credential Security Support Provider (CredSSP) either through TLS or Kerberos. NLA can also help to protect against man-in-the-middle attacks, where credentials are intercepted. However, be aware that NLA over NTLM does not provide strong authentication and should be disabled in favor of NLA over TLS (with valid certificates).

Microsoft TechNet describes configuration and usage of NLA in Windows Server 2008 R2 here.

Interestingly, BlueKeep, mentioned above, is partially mitigated by having NLA enabled. As reported by Microsoft in the associated advisory “With NLA turned on, an attacker would first need to authenticate to Remote Desktop Services using a valid account on the target system before the attacker could exploit the vulnerability.”

Restrict users who can logon using RDP

All administrators can use RDP by default. Remote access should be limited to only the accounts that require it. If all administrators do not need remote access you should consider removing the Administrator account from the RDP access group. You can then add the specific users which require access to the “Remote Desktop Users” group. See here for more information on managing users in your RDS collection.

Minimize the Number of Local Administrator Accounts

Local administrator accounts provide an attack vector for attackers who gain access to a system. Credentials can be cracked offline and more accounts means more likelihood of a successful crack. Therefore, you should aim for a maximum of one local administrator account which is secured appropriately.

Ensure that Local Administrator Accounts are Unique

If the local administrator accounts match those assigned to their counterparts on other systems within the server’s internal network, the attacker can potentially re-use credentials to move laterally. This issue occurs quite frequently, so Microsoft provided Local Administrator Password Solution (LAPS) as a means to avoid this scenario across the organization with central management of unique local administrator credentials. This is particularly relevant for externally exposed systems.

Microsoft provides a download and usage information for LAPS here.

Limit Domain Administrator Account Access

Accounts within the domain admins group have full control of the domain by default, by virtue of being part of the administrators group for all domain controllers, domain workstations and domain member servers. If a credential for a domain admin account is

retrieved from the RDP server, the attacker now holds the 'keys to the kingdom' and is in full control of the entire domain. You should reduce the amount of domain administrators within the organization in general and avoid accessing the RDP server or other externally exposed systems via these accounts, to avoid inadvertently making credentials accessible.

In general, 'least privilege' administration models should be used. Microsoft provides guidance in this area, including how best to use domain admin accounts, here.

Consider Placement Within the Network

Where possible, RDP servers should be placed within a DMZ or other restricted area of the network. The idea here is that if an attack is successful, its scope is reduced and confined to the RDP server alone. Often RDP is exposed specifically to allow external users onto the network, so this may not be a feasible solution, however it should be considered and the quantity of services reachable within the internal network should be minimized.

Consider using an account-naming convention that does not reveal organizational information

There are many options for account naming conventions, ranging from firstname.lastname to not deriving usernames from name data; all having their pros and cons. However, some of the more commonly used account naming conventions such as firstname.lastname, make it very easy to guess usernames and email addresses. This can be a security concern as spammers and hackers will readily use this information.

Conclusion

When trying to run an efficient IT organization, having remote access to certain computer systems might be essential. Unfortunately, when not implemented correctly, the tools that make remote access possible also open your systems up to unwanted guests. In the last few years there have been far too many examples of where vulnerable RDP access gave way to a full-scale network compromise.

In this article we have shown that RDP access can be hardened with some easy steps. Please take the time to review your RDP security posture.

About the Author

Darren Fitzpatrick

Darren is a Security Researcher on the McAfee Advanced Threat Research (ATR) team. With a focus on red teaming and with a particular interest in Active Directory attacks, Darren is passionate about breaking networked things to help make defensive blue teams stronger. Having transitioned to ATR from McAfee product engineering, red team work also feeds ...

Read more posts from Darren Fitzpatrick ›

John Fokker

John Fokker is a Principal Engineer and Head of Cyber Investigations for the Advanced Threat Research. Prior to joining the team, he worked at the National High Tech Crime Unit (NHTCU), the Dutch national police unit dedicated to investigating advanced forms of cybercrime. Within NHTCU he led the data science group, which focused on threat ...

Read more posts from John Fokker ›

Eamonn Ryan

Eamonn Ryan is a Security Researcher on the McAfee Advanced Threat Research team. Eamonn possesses both offensive and defensive skill sets but currently focuses on red team operations and adversary emulation. Eamonn specializes in defense bypass and evasion techniques with a focus on process manipulation.

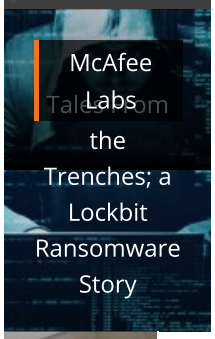
Read more posts from Eamonn Ryan ›

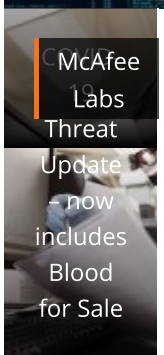
‹ Previous Article

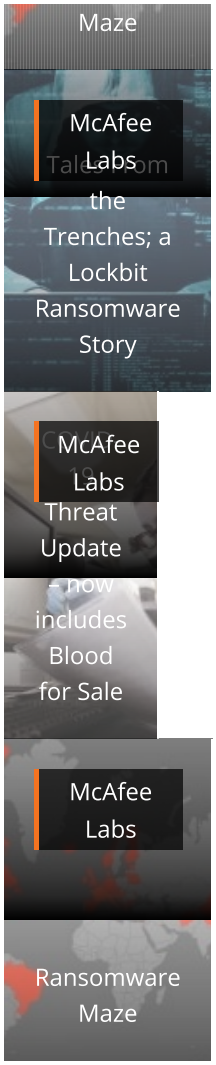
Next Article ›

Categories: McAfee Labs
Tags: Advanced Threat Research

Similar Blogs







Subscribe to McAfee Securing Tomorrow Blogs

Email address

Subscribe