The security risks of RDP

RDP, or Remote Desktop Protocol, is one of the main protocols used for remote desktop sessions. That's when employees access their office desktop from another device.

RDP is included with most Windows operating systems and can be used with Macs as well. Many companies rely on RDP to allow their employees to work from home.

A vulnerability is a bug in the way a piece of software is built that allows attackers to gain unauthorized access. Think of this as an improperly installed latch on the front door of a house, allowing criminals to break in.

These are the most important vulnerabilities in RDP:

1. Weak user credentials

Most desktops are password protected, and users can usually set this password to whatever they want. The problem is that users often use that same password for RDP remote login as well. Companies often don't manage these passwords to ensure their strength, and they often leave these remote connections open to Brute Force or Credential Stuffing attacks.

2. Unlimited port access

RDP connections almost always take place on port 3389*. Attackers can assume this is the port being used and target it to carry out attacks.

> * In a network, a gateway is a logical, software-based, location assigned to certain types of connections. Assigning different processes to different ports helps the computer keep track of those processes. For example, HTTP traffic always goes to port 80, while HTTPS traffic goes to port 443.

What are some ways to address these RDP vulnerabilities?

Single Sign On (SSO)

Many companies have used SSO services to manage user credentials for a variety of applications. SSO provides companies with an easier way to enforce the use of strong passwords, as well as implement more secure measures like two-factor authentication (2FA). RDP remote access can be moved out after the SSO process to work around the user login vulnerability described above.

Manage and enforce passwords

For some companies, moving RDP remote access out after the SSO process may not be an option. At a minimum, these companies should require employees to reset their desktop passwords to something stronger.

Gate lock 3389

Secure tunneling software can help prevent attackers from sending requests to port 3389. With a secure tunneling, any requests that don't go through the tunnel are blocked.

Firewall rules

The corporate firewall can be configured manually so that no traffic to port 3389 can pass through, except traffic from allowed ranges of IP addresses (for example, known to belong to the employee).

However, this method takes a lot of manual work and remains vulnerable if attackers take over an authorized IP address or an employee's device is compromised. In addition, it is often difficult to identify and allow pre-listing of all employee devices, leading to persistent IT requests from employees being blocked.

What other vulnerabilities does RDP have?

RDP has other vulnerabilities that are technically patched, but still serious if left unchecked.

One of the most critical vulnerabilities in RDP is called "BlueKeep". BlueKeep (officially classified as CVE-2019-0708) is a vulnerability that allows attackers to execute any code they want on a computer, if they send a specially crafted request to the correct port (usually is 3389). BlueKeep is capable of spreading the worm, which means it can spread to all computers in the network without any action from the user.

The best defense against this vulnerability is to disable RDP unless it's necessary. Blocking port 3389 using a firewall can also help. Finally, Microsoft released a patch to fix this vulnerability in 2019 and it is essential for system administrators to install this patch.

Like any other program or protocol, RDP also has a number of other vulnerabilities, and most of these can be eliminated by always using the latest version of the protocol. Vendors typically patch vulnerabilities in each new software version they release.