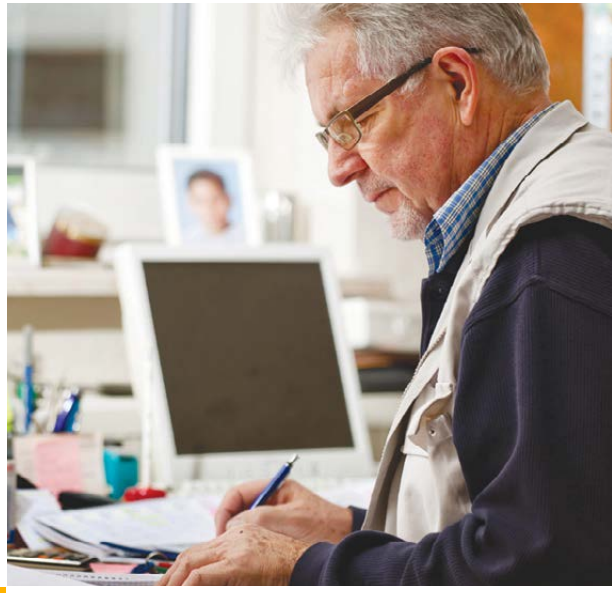
securityMETRICS®

White Paper

SECURING YOUR REMOTE DESKTOP CONNECTION

HOW TO PROPERLY SECURE REMOTE ACCESS



SECURING YOUR REMOTE DESKTOP CONNECTION

HOW TO PROPERLY SET-UP REMOTE ACCESS

INTRODUCTION

Remote computer access is now part of everyday work, allowing employees to access work files from home, airplane terminals, customer service centers, abroad, or anywhere there's an Internet connection.

Some remote access applications include:

- Windows Remote Desktop
- Apple Remote Desktop
- pcAnywhere (Symantec)
- Laplink Gold
- GoToMyPC
- LogMeIn
- TeamViewer
- Join Me
- UltraVNC
- TightVCN
- RDP

While remote computer access is a convenient and important technology, it's unfortunately also one of the most hacked business resources in recent years.

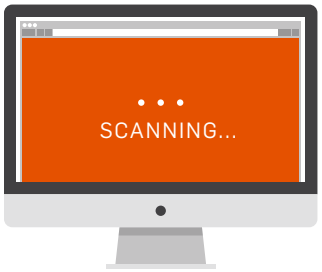
In 2014, SecurityMetrics PCI forensic investigators again confirmed that remote access was the top avenue attackers utilized to gain access into merchant systems. 80% of investigated merchants were attacked through insecure remote access applications. Of those compromised through remote access, 94% had cardholder data exfiltrated from their system by an attacker.

TOP REMOTE ACCESS VULNERABILITIES

It's not the remote access application itself that's inherently insecure; it's the manner in which remote access is configured. If not properly secured, remote access puts merchants at risk.

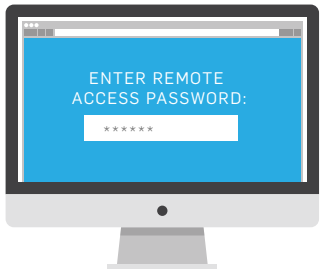
It allows attackers to bypass the firewall and most other system security measures to gain access to all systems within that network segment, which often includes the payment environment.

This is just one of the many examples of how an attacker could infiltrate a vulnerable remote access application:

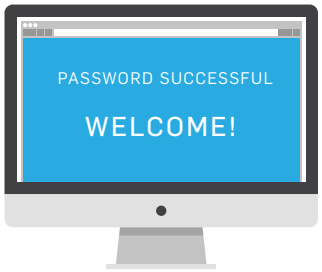


1. Scan the Internet for open remote access ports

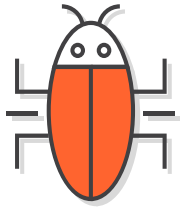
2. Use an online password list to brute force remote access credentials



3. Test remote access credentials



4. If credentials are successful, gain complete access to the system



5. Download malware onto the system

6. Capture sensitive data (e.g., credit cards, patient information, etc.)

Attackers will routinely scan large ranges of IP addresses looking for open ports that typically relate to the use of remote access tools (i.e., if attackers see that an IP address has ports 5800 and 5900 open, they assume that Virtual Network Computing (VNC) is installed. If they see that ports 5631 and 5632 are open, they assume the system is configured for pcAnywhere).

The attacker then tries a number of typical usernames that are commonly found on most systems, such as "admin" or "administrator," and then runs password-cracking tools in order to obtain the system administrator's or other user's password. Once attackers have obtained remote access credentials, they have system access and the ability to attack an environment, perhaps by uploading malware or copying sensitive data.

IF A REMOTE ACCESS APPLICATION CONFIGURATION ONLY REQUIRES THE USER TO ENTER A USERNAME AND PASSWORD, THE APPLICATION HAS BEEN CONFIGURED INSECURELY.

IMPROVING REMOTE ACCESS INSTALLATION

Remote access, and other applications, are often installed and used without changing the application's default password. Using default passwords to access these applications increases the likelihood of compromise.

Often, merchants are unaware that default settings continue to be used after installation. Data security weaknesses introduced to a merchant's system by third-party providers/vendors, such as IT Support and point of sale (POS) vendors is a growing concern.

Merchants trust that the third-party provider will configure their systems securely. But if the third-party provider fails to change default passwords and implement two-factor remote access authentication and there is a data breach, the merchant is at fault. Implementing these changes will later be discussed.

In October 2015, Visa announced new requirements for device installation and integration. Acquirers must require "all newly boarded Level 4 merchants to use only" PCI certified QIR professionals by March 31, 2016, and acquirers must "ensure that all existing Level 4 merchants use certified QIR professionals" by January 31, 2017.

In one SecurityMetrics forensic investigation, it was discovered that a third party IT vendor purposely left POS system default passwords in place to facilitate easier future system maintenance. Default passwords might make it easier for IT vendors to support a system without having to learn a new password each time; but convenience is never a valid reason to forego security, nor will it defray liability.

Most default passwords and settings are well known throughout hacker communities and are easily found via a simple Internet search. When defaults aren't changed, it provides attackers an easy gateway into a system. Disabling vendor defaults on every system with exposure to a cardholder data environment protects against unauthorized users.

STRENGTHENING PASSWORDS AND USERNAMES

If a username and password aren't sufficiently complex, it will be that much easier for an attacker to gain access to an environment. They may try to brute-force attack a system by entering multiple passwords (usually via an automated mechanism that allows them to enter thousands of password options within a matter of seconds) until one works.

Secure passwords should have a minimum of eight characters, and must contain numeric and alphabetic, and special characters. In practice, the more character formats used, the more difficult a password will be to guess. This also applies to attackers trying to use an algorithm to obtain a password: the longer, more complex the password, the longer it will take to discover.

Consider using a passphrase as your password. Passphrases are good because they are complex and easy to remember. For example, pick a phrase like "I like almonds in the morning" and add in some numbers and special characters. Your passphrase might look like "iLaitM183$"

Instead of common usernames such as "admin," administrator, company name, or a combination of the two, merchants should utilize fictitious names or a combination of characters, symbols, and numbers that don't fit the standard username.

IN 2014, NONCOMPLIANCE WITH PCI DSS REQUIREMENT 8 (ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS) CONTRIBUTED TO A MERCHANT'S COMPROMISE OR LOSS OF DATA IN 67% OF INVESTIGATED CASES.

ENABLING TWO-FACTOR AUTHENTICATION

Two-factor authentication is the most effective solution to secure remote access applications and is a requirement under PCI DSS. Unfortunately, merchants often fail to implement two-factor authentication.

Configuring two-factor authentication requires two of the following three factors:

- Something only the user "knows" (e.g., a username and password)
- Something only the user "has" (e.g., a cell phone, bar code, or an RSA SecureID token)
- Something the user "is" (e.g., a fingerprint, ocular scan, voice print, or other biometric)

A few examples of effective two-factor authentication remote access authentication include:

1. The remote user enters their username and password, and then must enter an authentication code that is sent to them on their cell phone.
2. Access to the remote access application is blocked to the outside. The remote user must call in to the location and speak with an authorized manager who recognizes them by voice. The onsite manager then opens a remote session. The remote user must then enter their username and password.

SYSTEM SECURITY SHOULD NOT BE BASED SOLELY UPON THE COMPLEXITY OF A SINGLE PASSWORD. NO PASSWORD SHOULD BE CONSIDERED UNCRACKABLE. PASSWORDS SHOULD ROUTINELY BE CHANGED AT LEAST EVERY 90 DAYS.

SECURING YOUR REMOTE ACCESS

It's critical to look at how to effectively govern company use of remote access technologies. When implemented and managed properly, remote access can be secure.

Here are a number of additional best practices recommended to protect your organization against hackers:

- **Limit those who can access the system remotely.** Only provide remote access to those whose job requires it. Don't share remote access credentials, and ensure everyone has a unique username and password.
- **Keep firewalls updated.** This helps ensure inbound rules provide adequate protection.
- **Maintain PCI compliance.** If you aren't already, implement and maintain PCI standards for continuing data security protection.
- **Get everyone on the same page.** Periodically review data security practices to ensure employees protect sensitive patient data.
- **Store and monitor logs.** Monitoring log activity can help identify suspicious activity alerts, such as if someone tried logging in at 3 a.m. over 300 times.
- **Run vulnerability scans.** These scans allow organizations to find and fix both internal and external vulnerabilities in a timely manner.
- **Don't allow guest accounts.** Guest accounts allow anonymous computer and system access. Disabling these accounts protects against unauthorized users.
- **Limit login attempts.** Set your remote access to lock out a user after six failed login attempts, with administrators able to unlock accounts.

Merchants should also keep third-party vendors' access to a minimum and monitor it regularly. This can be accomplished by a second authentication factor that requires the third-party to telephone the site and speak with an authorized manager who knows the vendor. The on-site manager may then authorize a temporary remote session for the vendor. When the vendor's work is complete, the on-site manager will then terminate the remote access.

CONCLUSION

Insecure remote access continues as the top vulnerability, but can be prevented through a few additional security measures.

Because of the prevalence of high-quality password-cracking tools, creative usernames and complex passwords are essential, but not enough. Strong two-factor authentication must also be implemented to ensure a safer remote access atmosphere.

Change default or insecure usernames and passwords for necessary services enabled on firewalls in order to make it more difficult for an attacker to gain access to your systems.

If a third party IT company is accessing the cardholder environment, it's still the responsibility of the merchant to ensure compliance. Check with third party companies to verify that any remote access applications have been securely configured.

ABOUT SECURITYMETRICS

SecurityMetrics has helped over 800,000 organizations comply with PCI DSS, HIPAA, and other mandates. Our solutions combine innovative technology that streamlines compliance validation with the personal support you need to fully understand compliance requirements.

CONSULTING@SECURITYMETRICS.COM

801.705.5656