VISA SECURITY ALERT

July 2014

INSECURE REMOTE ACCESS AND USER CREDENTIAL MANAGEMENT

Distribution: Acquirers, Merchants
Who should read this: IT, Information Security, IT Support

Summary

To promote the security and integrity of the payment system, Visa is committed to helping clients and payment system participants better understand their responsibilities related to securing cardholder data and protecting the payment industry. As part of this commitment, Visa issues Security Alerts when threats and vulnerabilities are identified in the payment system. Visa has recently observed an increase in malicious remote access activity associated with unauthorized access to merchant Point-of-Sale (POS) environments and ultimately, payment card data.

Insecure Remote Access

A number of remote access solutions are commonly used to provide remote management and support for retailers (e.g., LogMeIn, PCAnywhere, VNC, and Microsoft Remote Desktop). Used correctly, remote management applications are an effective method of providing technical support among large numbers of merchants. Used maliciously, they potentially expose payment card data and other sensitive information to cybercriminals. Insecurely deployed remote access applications create a conduit for cybercriminals to log in, establish additional "back doors" by installing malware, and steal payment card data. The risk of data compromise is increased when remote access applications are configured in a manner that does not comply with the Payment Card Industry Data Security Standard (PCI DSS).

The following are examples of common remote access vulnerabilities that can enable intruders to gain access to merchant POS environments. Please note that most of these are also violations of the PCI DSS.

- **Remote access ports and services always available on the Internet.** An intruder only needs to perform a port scan against a merchant's IP address space to identify potential targets of opportunity. Remote access applications often run on predictable, well-known ports.

- **Outdated or un-patched applications and systems.** Older versions of application and operating system software are known to be susceptible to attack and are easily exploited to gain unauthorized access.

- **Use of default passwords or no password.** Using default settings and passwords to access system components will increase the likelihood of a compromise. New hardware devices and software generally arrive from vendors configured with default settings. These default settings must be changed prior to production deployment, as they can be easily guessed and information about these settings is readily available on the Internet.

- **Use of common usernames and passwords.** Often, a vendor or service provider will use a common username and password at multiple client locations to facilitate service calls.

- **Single-factor authentication.** Remote access can be vulnerable to brute force and password-guessing attacks**,** particularly when authentication only requires a username and password.

- **Improperly configured firewalls.** In some cases, the POS system has a public IP address that is directly accessible from the Internet.

Compromised Remote Access Credentials

An investigation of a series of leads from recent attacks against merchants throughout the United States, pointed to a common threat involving remote access software operating in the merchant POS environment. Attacks were suspected to have occurred as a result of compromised username/login credentials combined with remote management software exposed to the Internet. The circumstances around multiple merchant compromises in the last several months suggest an actor or group of actors are targeting merchants who share common POS integrators or remote support vendors.

The attacks take place by successfully logging in to remote access applications, presumably using common username/password combinations that are shared among large groups of merchants. Once inside the merchant's network, an intruder will typically take steps to disable anti-virus applications and establish additional “back door” connectivity through the installation of malicious software (malware). On systems where payment card data processed, card-capturing malware is often installed and used to collect full track data from the POS system. Finally, card data is exfiltrated to remote IP addresses.

Mitigation

Visa strongly urges merchants and payment system stakeholders to share this alert with their POS vendors, resellers and integrators. To address this threat, examine remote management software for insecure configurations, use of outdated or unpatched applications, common or easily-guessed usernames and passwords, and ensure that overall payment processing environment is securely configured and maintained in accordance with the PCI DSS.

Additionally, the following security practices will help mitigate security risks:

- Ensure proper firewalls rules are in place, only allowing remote access only from known IP addresses.
- If remote connectivity is required, enable it only when needed.
- Contact your support provider or POS vendor and verify that a unique username and password exists for each of your remote management applications.
- Use the latest version of remote management applications and ensure that the latest security patches are applied prior to deployment.
- Plan to migrate away from outdated or unsupported operating systems like Windows XP.
- Enable logging in remote management applications.
- Do not use default or easily-guessed passwords.
- Restrict access to only the service provider and only for established time periods.
- Only use remote access applications that offer strong security controls.
- Always use two-factor authentication for remote access. Two factor authentication can be something you *have* (a device) as well as something you *know* (a password).

Additional Resources

- PA DSS Security Requirements

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Canada Region, Latin America Region, United States: USFraudControl@visa.com

For more information, please contact Visa Risk Management: cisp@visa.com