Risk Management | Fraud Alert 19 April 2011

Visa Security Alert: Remote Access Vulnerabilities—Most Frequent Attack Method Used by Intruders

AP, Canada, CEMEA, LAC, U.S.

Acquirers and processors, please share this alert with your merchants as soon as possible. Translated versions will be available in the Visa Publication Center within four business days.

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 as a reminder of best practices or when emerging vulnerabilities are identified in the marketplace.

Remote Access Vulnerabilities

Insecure remote access continues to be the most frequent attack method used by intruders to gain access to a merchant's point-of-sale (POS) environment. There are a variety of remote access solutions available, ranging from command-line based (SSH, Telnet) to visually driven packages (pcAnywhere, VNC, MS Remote Desktop). **Note:** Remote management applications come with an inherent level of risk, creating a virtual "back-door" for unauthorized access; therefore, these applications must be configured in a manner that complies with the Payment Card Industry Data Security Standard (PCI DSS).

The exploitation of improperly configured remote management software tools is the method of attack most frequently used by hackers against POS payment systems. Most merchants rely on third parties (POS vendors, resellers or integrators) to manage their POS systems. It is important that merchants require that these third parties follow established best practices when remotely accessing POS systems.

Visa has identified these examples of common remote access vulnerabilities, which allow intruders to gain access to merchants' POS environments:

- **Remote access ports and services always listening from the Internet.** An intruder only needs to perform a port scan on a merchant's IP address to identify available ports.
- **Use of default password or no password.** Often, a vendor's password is used at multiple merchant locations.
- **Lack of two-factor authentication.**
- **Lack of a properly configured firewall.** In some cases, the POS system has a public IP address that is directly accessible from the Internet.

Once an intruder is inside a merchant's network, the intruder can install malicious software (such as key logger malware or packet sniffers) to capture full track data from the POS system and exfiltrate data to the intruder's IP address(es).

Recommended Mitigation Strategy

Visa strongly urges merchants and stakeholders to share this alert with their POS vendors, resellers and integrators; review remote management software for insecure configurations and weak passwords; and ensure that networks and the overall payment environment are securely configured and maintained in accordance with the PCI DSS.

Additionally, the following security practices should be implemented to help mitigate security risks:

- Disable remote access from the Internet.
- If remote connectivity is required, secure remote access by turning on remote access only when needed.
- Do not use default or trivial passwords.
- Only use remote access applications that offer strong security controls.
- Always use two-factor authentication.
- Restrict access to third party sites; restrict authentication credentials only to third parties who need access.
- Limit access to a specific number of trusted IP addresses.
- Use the latest version of a remote management product or service; ensure that the latest security patches are applied prior to full deployment.
- To protect data transmissions between the POS system and a remote PC, enable data encryption within the remote management system.
- Enable logging into remote management products, operating systems, firewalls and any other devices that support logging. (Audit logs are valuable in the event of suspected unauthorized activity and for monitoring of traffic patterns within your network. Logs also play an integral role in identifying illegitimate traffic, as well as scoping the extent of a possible compromise.)
- Implement a hardware-based stateful firewall. (Stateful firewalls keep track of the state of a network connection; only packets matching a known connection state are permitted by the firewall.)

If you detect a security breach, notify your acquiring bank immediately. You can also contact Visa Fraud Control using the contact information provided below:

- **Visa U.S. region:** Call (650) 432-2978 or e-mail USFraudControl@visa.com
- **Visa Canada region:** Call (416) 860-3090 or e-mail CanadaInvestigations@visa.com
- **Visa Latin America and Caribbean (LAC) region:** Call (305) 328-1713 or e-mail lacrmac@visa.com
- **Visa Asia Pacific region:** Call (65) 96307672 or e-mail APInvestigations@visa.com
- **Visa Central and Eastern Europe, Middle East and Africa (CEMEA) region:** Call +44 (0) 207-225-8600 or e-mail CEMEAFraudControl@visa.com

Related Documents

What To Do If Compromised: Visa Inc. Fraud Control and Investigations Procedures.

For More Information

For more information or to ask questions about the information in this alert, please visit www.visa.com/cisp (see "Alerts & Bulletins") or e-mail USFraudControl@visa.com.