

Visa Data Security Bulletin

Improperly Segmented Network Environment

July 2, 2009

To promote the security and integrity of the payment system, Visa is committed to helping financial institutions 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 Data Security Bulletins when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Financial institution clients may share this bulletin with their stakeholders to help ensure they are aware of these emerging vulnerabilities and take steps to mitigate risks.

Security Vulnerability

Improper Segmented Network Environment

Payment card account information has been compromised at merchant locations that lack proper network segmentation. This attack method originates on the Internet, results in penetration of the merchant's Point of Sale ("POS") system and often results in costly remediation efforts and increased fraud attacks. Such compromises can often be prevented if the merchant networks are properly segmented so that intruders are limited to non-sensitive parts of the POS network that do not contain payment card information.

Network segmentation is a concept that refers to the practice of splitting a network into functional segments and implementing an access control mechanism between each of the boundaries. The most common example of network segmentation is the separation between the Internet and an internal network using a firewall/router.

Merchants are reminded that when e-mail and web browsing are introduced to their networks, a potential avenue of attack can be opened. A malicious e-mail attachment or a malicious web page can introduce viruses, spyware and malware into an internal network. Once such harmful software is within the boundaries of your internal "trusted" network, it allows uninhibited access to all devices on the network.

This scenario can be abused to gain access from a user system to a business (payment-processing) system and result in data loss.

Recommended Mitigation Strategy

To comply with Payment Card Industry Data Security Standards (PCI DSS) requirements, adhere to the following recommendations:

- Separate any user environments from any business systems using a firewall. For example, a system used by employees to receive e-mail should be separated from a system used for transaction processing.
- Configure the firewall to only allow access between systems participating in the transaction flow. Further limit the allowed host connections to the Wi-Fi access point by specifying individual MAC or IP addresses.
- Limit access to only network ports that are necessary to perform desired business functions.
- Access controls should be applied to both directions of network traffic – inbound and outbound.
- Enable logging and exception alerting on all network devices and business systems, where possible. Log files should be protected from tampering. Logging is an essential tool in analyzing the current state of your network, and can identify and scope potential intrusions.
- Use a Virtual Private Network ("VPN") or Secure Sockets Layer ("SSL") connection between systems processing sensitive data whenever possible. Connections utilizing encryption ensure the confidentiality and integrity of the data by protecting it against eavesdropping.
- Implement a switched network – switches handle network traffic in a manner more resistant to eavesdropping.

For more information or questions regarding the information in this bulletin, please visit www.visa-asia.com/secured or e-mail vpssais@visa.com.