VISA

Visa Data Security Alert

Potential Network Vulnerabilities for Financial Institutions

January 25, 2008

WARNING - PLEASE READ IMMEDIATELY

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 Alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

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

Security Vulnerability

Potential Network Vulnerabilities for Financial Institutions

Visa Fraud Investigations and Incident Management has identified incidents where financial institutions have been targeted by hackers seeking sensitive cardholder information. These institutions are reminded that Web-facing systems may be susceptible to a network breach if not properly secured. Web-facing systems can become entry points for hackers seeking cardholder information, and breaches of these systems can introduce malicious software ("malware") into critical internal networks. Visa has observed incidents where hackers have been able to penetrate an internal network through the following exploits:

- Establishing continuous remote access to the internal network through a "back door"

- Compromising internal systems passwords using a password-cracking program

- Mapping the internal network infrastructure

To guard against these recently observed exploits, financial institutions should review the network vulnerabilities identified below and implement mitigating controls where appropriate.

1. Failure to use a Network-Based Intrusion Detection System

Network-based intrusion detection systems (NIDS) are designed to monitor network traffic in order to distinguish between 'normal' network activity and 'abnormal' or 'suspicious' activity that may identify an attack. The early detection of a network compromise is difficult without adequate network monitoring and intrusion detection capabilities. successful compromise include:

- Unexpected outbound transmission of sensitive data

- Network connections originating from internal critical systems that would not normally communicate outside the network, including untrusted networks and the

Without the means to detect suspicious events on a host system or critical files, unauthorized access by a user or malware can remain undetected.

Risk Mitigation Strategy:

Implement HIDS on critical systems, particularly those that involve the flow of payment card data, to monitor for suspicious or anomalous events.

3. Improperly segmented network environment

Payment card account information can be compromised at financial institutions or merchant locations that lack proper network segmentation.

 Alert 012508

For more information, please refer to the October 31, 2006, Visa Data Security Brief, "Improperly Segmented Network Environment," available online at http://usa.visa.com/merchants/risk_management/cisp_alerts.html.

4. Poorly configured ingress and egress firewall rules

Firewall ingress (inbound) and egress (outbound) rules that are misconfigured or left unchanged from their default configurations represent an area of significant vulnerability. For more information on ingress and egress firewall rule misconfiguration, please refer to the *Visa Business Review* article (Issue No. 070911), "Visa Identifies Top Network Vulnerabilities to Promote Data Security Awareness," available at https://www.us.visaonline.com.

5. SQL injection

A review of recent data security breaches suggests Structured Query Language (SQL) injection attacks on e-commerce Web sites and Web-based applications that manage card accounts (e.g., PIN updates, monetary additions, account holder updates) have become more prevalent.

SQL injection attacks are caused primarily by applications that lack input validation checks, un-patched Web servers and poorly configured Web and database servers. These attacks pose serious additional risks to cardholder data stored or transmitted within systems and networks connected to the affected environment. For more information on SQL injection, please refer to the Visa Data Security Alert, "SQL Injection Attacks," also attached to this alert e-mail.

For more information or questions regarding the information in this alert, please visit www.visa.com/cisp or e-mail cisp@visa.com.

Alert 012508