To promote the security and integrity of the payment system, Visa is committed to helping Visa clients, service providers and merchants better understand how they can best protect their businesses and customers. As part of this commitment, Visa provides data security alerts focused on the most common security vulnerabilities, attack methods and emerging risks identified in the payment system. The alerts also include guidance and best practices stakeholders can follow to mitigate the risk of compromise.

Visa Data Security Alert

January 2013

ATM Cash-Out Fraud Cases

Audience: Issuers/Processors/ATM Acquirers
Category: Technical (IT, Information Security)

Visa has been alerted to new cases where ATM Cash-Out frauds have been attempted and successfully completed by organized criminal groups across the globe. In a recently reported case, criminals used a small number of cards to conduct 1000's of ATM withdrawals in multiple countries around the world in one weekend.

International Law Enforcement Agencies have information that suggests further attempts may be imminent and are warning issuers, especially of prepaid products, to increase monitoring of ATM traffic and report any suspect activity.

These attacks result from hackers gaining access to issuer authorization systems and card parameter information. Once inside, the hackers manipulate daily withdrawal amount limits, card balances and other card parameters to facilitate massive fraud on individual cards. In some instances over $500K USD has been withdrawn on a single card in less than 24 hours.

Hackers have been able to penetrate an internal network through the following exploits:

- Web-based vulnerabilities, such as SQL injection
- 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

Vulnerabilities and Recommended Mitigation Strategy

To prevent ATM Cash-Out fraud of this nature, ATM acquirers, processors and card issuers need to increase monitoring of ATM traffic and ensure that appropriate safeguards are in place. **ATM acquirers and processors** should review their transaction monitoring rules and where suspect activity is seen; take steps to immediately contact the issuer. **Card Issuers** should monitor ATM transaction velocity on issued cards and set monitoring rules that restrict excessive and suspect withdrawal amounts.

Below are a list of network vulnerabilities and mitigating controls that financial institutions should also review and implement 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 signal an attack. The early detection of a network compromise is difficult without adequate network monitoring and intrusion detection capabilities.

Risk Impact:
Without the means to detect suspicious network events, network compromises can remain undetected.

Risk Mitigation:
NIDS can detect and mitigate suspicious events when deployed in conjunction with full compliance with Payment Card Industry Data Security Standard and implementation of a robust security monitoring strategy.. Suspicious events that may be symptoms of a 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 Internet

2. Failure to utilize a Host-Based Intrusion Detection System

Host-based intrusion detection systems (HIDS) are designed to monitor the behavior of host / computer systems to distinguish between 'normal' activity and 'abnormal' or 'suspicious' activities. A key function of HIDS is to detect unknown activities caused by malware, packet sniffers or rootkits by monitoring incoming and outgoing communications traffic. HIDS will then check the integrity of critical system files and directories and watch for suspicious processes and executables.

HIDS can also monitor the usage of system accounts with elevated or administrative privilege. Unexpected or unexplained useage of accounts with administrative privilege is often a sign of a larger compromise.

Risk Impact:
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.

Risk Mitigation Strategy:
Ensure the Cardholder Data Environment (CDE) is segregated from the corporate network. If that cannot be done quickly, or the effectiveness of the segmentation is in question, conduct a pentest of the corporate environment to identify high risk vulnerabilities.

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.

Risk Mitigation Strategy:
Verify that a "deny all" rule exists in all firewalls, and that rules using unused ports are deleted.

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.

Risk Mitigation Strategy:
Older websites, especially Microsoft sites that predate .net should be upgraded or reviewed for security vulnerabilities. For more information on SQL injection, please refer to the Visa Data Security Alert, "SQL Injection Attacks," available at
http://usa.visa.com/download/merchants/Alert_SQL_Injection_20090901.pdf

For more information or to report any suspicious activity, please contact Visa Fraud Control at:

VIFraudControl@visa.com for APCEMEA
USFraudControl@visa.com for US, Canada and LAC