

Visa Inc. Data Security Alert

Network Vulnerabilities

June 19, 2008

In accordance with the Payment Card Industry Data Security Standard (PCI DSS) and to promote the security and integrity of the payment system, Visa Inc. is committed to helping clients and payment system stakeholders better understand their obligation to protect cardholder information. As part of this commitment, Visa issues Data Security Alerts when emerging vulnerabilities are detected in the marketplace.

Visa clients are strongly encouraged to share this alert with their merchants (particularly Level 1 and Level 2 merchants) and other payment system stakeholders to promote awareness of these threats and ensure immediate steps are taken to mitigate risk.

Network Security Vulnerability

Recent data security breaches reported to Visa indicates that Level 1 and Level 2 merchants remain common targets for data compromise. Hackers are successfully launching aggressive attacks against corporate networks and gaining access to payment card data using two prevalent methods: 1) Structured Query Language (SQL) injection, and 2) Packet Sniffing.

SQL Injection

SQL injection is a technique used to exploit e-commerce websites and web-based applications using client-supplied data in SQL queries. In recent security breaches investigated by Visa, forensic evidence revealed that corporate websites, commonly vulnerable to SQL injection attacks, were being exploited by hackers. These corporate websites traditionally consisted of company information (e.g., career search, press and investor resources, etc.) and often had no relation to sensitive data systems.

However, a single vulnerability at the corporate website could allow a hacker to infiltrate the company's core processing network and navigate to systems where sensitive customer data -- including cardholder data -- is stored or transmitted.

Packet Sniffing

Hackers who successfully gain access to a corporation's network may install a packet sniffer to eavesdrop or spy on network activity, log traffic passing over a computer

network and deploy malicious software. Ultimately, the use of an unauthorized sniffer on a corporation's network may result in the interception of payment card data.

Recommended Mitigation Strategy

Merchants (particularly Level 1 and Level 2 merchants) and other payment system stakeholders must remain vigilant about data security and safeguard against the compromise of Visa account information caused by SQL injection attacks and unauthorized packet sniffing. Entities are strongly urged to consider and implement the following risk mitigation strategies to counter internet attacks and protect cardholder data:

- **Adopt secure web-coding practices and hardening techniques that include:**
 - Independent code reviews and regular susceptibility testing against SQL injections (particularly for corporations that use proprietary custom applications)
 - Disabling unnecessary ports and functions such as xp_cmdshell, which are generally enabled by default and can issue operating system commands to database servers
 - Ensuring web and database servers are updated with current security patches
- **Prevent criminals from infiltrating and eavesdropping on corporate networks by taking steps to:**
 - Utilize host-based Intrusion Detection Systems (IDS)
 - Install and monitor firewalls for suspicious traffic (particularly outbound traffic) to unknown IP addresses and monitor event logs for failed attempts
 - Monitor user accounts (especially those with administrative level privileges) for unusual local and remote access dates, times and locations
 - Secure user workstations to ensure that packet sniffers or other malware cannot be installed
 - While not required by PCI DSS, consider encrypting transmission of sensitive data to protect and render "sniffed" data unreadable.

For more information on Visa's Cardholder Information Security Program, please visit <http://www.visa.com/cisp>.