Visa Data Security Alert

SQL Injection Attacks

January 25, 2008

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

SQL Injection Attacks

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 is a technique used to exploit Web-based applications that use client-supplied data in SQL queries. SQL injection attacks can occur as a result of un-patched Web servers, improperly designed applications (incorrectly filtered escape characters or error-type handling) or poorly configured Web and database servers.

The SQL attack methods most recently detected were targeted against Web sites and Web applications that were not properly designed or resided on un-patched systems, and were therefore susceptible to attack. These latest SQL injection attacks pose serious additional risks to cardholder data stored or transmitted within systems (e.g., Microsoft and UNIX-based) and networks connected to the affected environment.

Recommended Mitigation Strategy

To minimize the possibility of a SQL injection attack and mitigate the risk of a data compromise, merchants, issuers, acquirers, processors and agents should take the following actions:

- Use only a secure shopping cart validated by Visa's Payment Application Best Practices (PABP). A list of PABP-validated shopping carts is available on *www.visa.com/cisp*.

- Test susceptibility to SQL injection utilizing automated tools or manual techniques.

- Organizations that utilize proprietary or custom applications should adopt secure coding practices that include regular independent code reviews and testing against SQL injection.

- Use only secure Web and database servers. Please refer to product vendor Web sites for instructions on hardening Web and database servers (e.g., visit *www.microsoft.com* for instructions on hardening IIS Web servers and SQL database servers).

- Ensure all systems, including Web and database servers, are routinely updated with the current vendor security patches.

- Regularly monitor relevant information security alerts and ensure the latest vulnerabilities from industry resources are addressed (e.g., US-CERT, SANS).

- Purge cardholder data when no longer needed and take steps to ensure prohibited cardholder data (e.g., full magnetic-stripe data, CVV, CVV2, PIN-data) is not stored following transaction authorization.

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