CISP BULLETIN

Top Five Data Security Vulnerabilities Identified to Promote Merchant Awareness

August 29, 2006

The protection of cardholder account information is a responsibility that is shared by all participants in the Visa payment system. Visa is committed to providing educational information to members about potential vulnerabilities as they are identified. To promote compliance with the Cardholder Information Security Program (CISP) and the Payment Card Industry Data Security Standard (PCI DSS), Visa has identified the top five vulnerabilities detected in compromises.

Top Five Data Security Vulnerabilities Leading to Compromises

1. Storage of Track Data (and other sensitive data)

Track data is the information encoded and stored on two tracks located within the magnetic stripe on the back of a Visa card. The *Visa U.S.A Inc. Operating Regulations* and PCI DSS Requirement 3.2.1.4 explicitly prohibit the storage of the full contents of the magnetic stripe once the authorization process is completed. Unfortunately, many merchants and service providers may be unknowingly storing this data because a number of commercially available Point of Sale (POS) payment systems and custom-designed payment applications retain this data by default without any action by the user. Visa regulations and the PCI DSS also prohibit the storage of the Card Verification Value 2 (CVV2) and Personal Identification Numbers (PINs) or PIN blocks.

Risk Impact:

The value of full track data to hackers is significant. With little effort, a duplicate card can be created that will appear indistinguishable from the original card during the authorization process. Mass storage of this data by merchants and agents exposes this sensitive information to potential compromise and can make it easy for hackers to commit fraud that is difficult for issuers to detect. CVV2 and PINs are also highly sought after by hackers and when compromised can expose the payment system to undue risk.

Risk Mitigation Strategy:

Merchants that use commercially available POS systems should contact their POS vendors to validate whether the applications and versions in use are storing track data or other sensitive data, such as PINs. Additionally, merchants can ensure their payment applications do not store track data or other sensitive data by using a payment application that has been validated as compliant with Visa's Payment Application Best Practices program. The Payment Application Best Practices was created by Visa to help members and merchants comply with the PCI DSS

and Visa's CISP program. It facilitates compliance by establishing minimum standards to ensure payment applications are securely coded and do not retain track data. A list of Payment Application Best Practices compliant payment applications can be found at www.visa.com/cisp. Merchants that discover track data or other sensitive data in their systems should immediately delete this data and take steps to upgrade or replace any software vulnerable to this security flaw.

Custom-designed solutions should also be carefully evaluated for any evidence of magnetic-stripe data storage. If track data or other sensitive information is stored subsequent to an authorization, the data should be eliminated immediately and the solution modified to no longer store this data.

2. Missing or Outdated Security Patches

Hackers are constantly attempting to exploit known software vulnerabilities, as well as uncover unknown deficiencies in commercially available software products. Product vendors respond with frequent remediation measures in the form of software updates or patches. As specified in PCI DSS Requirement 6.1, it is imperative that all software updates or patches be applied as soon as possible to minimize the risk of compromise.

Risk Impact:

An improperly patched system offers an attacker a convenient method to exploit known vulnerabilities with minimal effort. Automated tools are constantly being developed by attackers to locate vulnerable systems. Moreover, a single exploitation of such a security gap can lead to the compromise of the merchant's payment system infrastructure and result in a large-scale loss of data.

Risk Mitigation Strategy:

The timely application of security patches is key to managing this vulnerability. Many vendors now offer automated alert services that provide prompt notification to their clients. Some vendors also provide automated patching mechanisms. If a patch cannot be applied immediately, other controls to mitigate this risk should be implemented, and monitoring of all affected systems should be increased. Merchants should establish software upgrade policies and procedures to ensure patches are reviewed and installed in a timely manner.

3. Vendor-Supplied Default Settings and Passwords

Hardware and software products come packaged from vendors with original default (or blank) settings and passwords for ease of installation and management. These settings and passwords are often not changed when they are deployed, which can create an opportunity for hackers to exploit. This practice violates PCI DSS Requirement 2.1, which requires that vendor-supplied defaults be changed before a system is installed on the network.

Risk Impact:

The default settings and passwords used to access hardware and software are easily guessed and often are well publicized in hacker chat rooms. Once an attacker accesses one of these systems, security mechanisms can easily be turned off, databases can be accessed and any evidence of an intrusion can be eliminated.

Risk Mitigation Strategy:

Any default or blank settings and passwords should be changed prior to deployment into production. Passwords should comply with current industry standards for storing passwords. Any default settings should be modified immediately. For example, default IDs should be renamed and default port numbers should be changed, where possible.

4. SQL Injection

SQL injection is a technique used to exploit Web-based applications by using client-supplied data in SQL queries. SQL injection attacks are caused primarily by applications that lack input validation checks. Recently, commercial shopping cart products have been the focus of attack by hackers who seek account information. PCI DSS Requirement 6.5 requires that Web-facing applications be developed in accordance with secure coding guidelines to guard against such attacks.

Risk Impact:

A successful SQL injection attack can have serious consequences. SQL injection attacks can result in the crippling of the payment application or an entire e-commerce site. Through this avenue of attack, an attacker can break out of the Web server and database realms, gaining complete control over the underlying system. Another serious consequence can be the compromise and theft of data that resides within the payment application infrastructure.

Risk Mitigation Strategy:

Any part of the payment application infrastructure that accepts client input and subsequently passes this data onto a database must validate the legitimacy of the input. Values not conforming to the expected and acceptable input criteria must not be allowed to pass this validation step.

Custom-coded payment applications should be reviewed for potential SQL injection-related weaknesses and should at a minimum adhere to the industry-defined secure coding standards. Automated tools are available in the marketplace to test applications for susceptibility to an SQL injection attack and should be utilized. Applications should not be permitted to submit dynamic SQL statements from the application layer to the database layer — stored procedures offer a greater level of security.

Merchants that utilize commercially available payment applications should ask their vendors to confirm whether the application adheres to the secure coding standards and whether a patching mechanism is provided to guard against potential weaknesses. Vulnerabilities for these products are often widely publicized within the hacker and security communities. Monitor the vendor's Web site, as well as security-related Web sites, to stay informed of new vulnerabilities specific to your product and version. Web servers that are utilized by merchants should be secured in accordance with their vendors hardening process.

Additionally, SQL firewalls have now been introduced to the marketplace and should be utilized whenever feasible. These hardware-based products are capable of making real-time, intelligent decisions based on a pre-defined or learned set of rules. For example, an SQL firewall allows for controlling the extent of any possible compromise by using rule-based connection resets, effectively terminating any offending connections to the data store. One of the secondary benefits that results from the usage of such tools is better insight into the behavior of users who connect to the data store, as well as a better understanding of the workload placed on the

system. Lastly, merchants can reduce the risk of SQL injection attack by only using a payment application that is compliant with Visa's Payment Application Best Practices. A list of Payment Application Best Practices compliant payment applications can be found at www.visa.com/cisp.

5. Unnecessary and Vulnerable Services on Servers

Servers are often shipped by vendors with additional services and applications that are enabled by default and may be unnecessary. These services may include tasks that run in the background and provide a specific type of functionality, such as carrying out database, FTP, e-mail, or Web-hosting related tasks. In today's environments, servers are usually dedicated to perform a limited set of tasks and should be hardened accordingly. For example, dedicated mail servers provide e-mail functionality and therefore have no need to run services such as FTP. Further, database servers already host data and may not have a need for a mail service. These unnecessary services should be disabled, as covered by PCI DSS Requirement 2.2.2, to minimize the risk of compromise.

Risk Impact:

Services or applications that are not needed may be ignored by the system administrator. As a result, software patches that would normally be installed to guard against known vulnerabilities may be ignored, thereby creating a means for hackers to gain access to the server. Successful exploitation of a vulnerability may result in an attacker gaining partial or complete control of the infrastructure. This may occur through the introduction of malware (viruses, Trojan horses, etc.) into the system and result in possible data theft or data destruction.

Risk Mitigation Strategy:

All necessary services or applications should be patched and secured. Any and all unused services or applications should be completely disabled or removed from all production environments. Disabling unnecessary services also may increase the system performance and improve stability due to lessened process contention and resource utilization.

For more information on Visa's Cardholder Information Security Program, please visit http://www.visa.com/cisp. Questions about this bulletin may be directed to CISP@Visa.com.