



Visa U.S.A. Inc. Data Security Briefs

April 18, 2007

To support compliance with the Payment Card Industry Data Security Standard (PCI DSS), Visa USA is committed to helping members and payment system participants better understand their responsibilities related to securing cardholder data. As part of this commitment, Visa issues security briefs when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Members may share this brief with their merchants, agents and other parties to help ensure they are aware of emerging vulnerabilities, and to take steps, where appropriate, to mitigate risk.

Security Vulnerability

Unnecessary and Vulnerable Services on Servers

As reported previously, compromises of Visa account information have occurred when hackers exploit vulnerabilities created when merchants do not disable 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 or redundant to the user. These services may include tasks that run in the background and provide a specific type of functionality, such as running database, File Transfer Protocol (FTP), e-mail or Web-hosting related tasks. In today's environment, one of Information Security's best practices includes dedicating servers to perform a limited set of tasks and securing them 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. Therefore, these unnecessary services should be disabled, as covered by PCI DSS Requirement 2.2.2., to minimize the risk of compromise.

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.

Recommended Mitigation Strategy

To safeguard against the compromise of Visa account information caused by unnecessary and vulnerable services on servers, merchants and agents should take the following actions:

- All necessary services or applications should be patched and secured.
- All unused services or applications should be completely disabled or removed from all production environments.

Please also note that, in addition to securing Visa account data, disabling unnecessary services may increase 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>