

# Critical Vulnerabilities Identified to Alert Payment System Participants of Data Compromise Trends

Please be advised that Visa has introduced Critical Vulnerabilities for U.S. merchants.

To support compliance with the Payment Card Industry Data Security Standard (PCI DSS), Visa has outlined essential security practices to mitigate the following data security vulnerabilities. These measures, on their own, may not be appropriate or sufficient depending on the implementation of an entity's information technology (IT) infrastructure and business needs. As such, Visa provides this information solely to build awareness of data security and industry best practices. It is important that all payment system participants continue to be diligent and maintain PCI DSS compliance at all times.



## Top Five Data Security Vulnerabilities Leading to Compromises

### 1. SQL Injection

Structured Query Language (SQL) injection is a technique used to exploit web-based applications and websites integrated with a database that uses user-supplied data in SQL queries. SQL injection attacks can occur as a result of unpatched web servers, improperly designed websites and applications, or poorly configured web and database servers. Using this method, an attacker can cripple a web application or an entire website and gain complete control over the underlying operating system. Another serious consequence can be the compromise and theft of data that resides within the web application, website environment or any connected systems across the network.

Common SQL injection attack techniques include form field manipulation and URL manipulation. Form field manipulation can be exploited anywhere that user-supplied data is entered into a website,

and is often found in dynamic pages, shopping carts, data input forms and login pages. URL manipulation is a method of altering a website address by modifying the web application parameter name and value pairs. Corporate websites are often vulnerable to these attacks as the corporate entity may not understand the web environment and its ability to directly or indirectly access cardholder data.

### **Risk Mitigation Strategy**

To minimize the possibility of a SQL injection attack and mitigate the risk of a data compromise, payment system participants should take the following actions:

#### PCI DSS Requirements 2 and 3

- *Use only secure web and database servers. For instructions on hardening web and database servers, please refer to product vendor websites.*
- *Programmatic functions used to execute operating system (OS) commands through stored procedures SQL statements, often setup by default, should be disabled to minimize risks (e.g., xp\_cmdshell).*
- *Purge cardholder data when it is no longer needed and take steps to ensure that prohibited cardholder data (i.e., full magnetic-stripe, CVV2 or PIN data) is not stored following the authorization of a transaction.*

#### PCI DSS Requirement 6

- *Ensure that all systems, including web and database servers, are routinely updated with the most current security patches available from their vendors.*
- *Organizations that utilize proprietary or custom applications should adopt secure coding practices that include independent code reviews and regular testing against SQL injection.*
- *Test susceptibility to SQL injection utilizing automated tools and manual techniques.*
- *Sanitize input data by checking for known and expected data by type, length, format and range.*
- *Do not display detailed error messages to an end user or expose information that can be used to breach a database system. Instead, log detailed error messages for internal troubleshooting and security review purposes.*
- *Use properly configured web applications or SQL firewalls.*

#### PCI DSS Requirements 7 and 12

- *To prevent access to the operating system, enforce least privileged database accounts that are necessary for web application use.*
- *Regularly monitor relevant information security alerts and ensure that the latest vulnerabilities from industry resources are addressed (e.g., US-CERT, SANS).*

## 2. Unpatched and Unhardened Systems

Hackers continually attempt to exploit known operating system and software vulnerabilities, as well as uncover unknown deficiencies in commercially available software products. Additionally, for ease of installation and management, new hardware devices and software generally arrive from vendors preconfigured with default, blank or weak security configuration settings. Examples of devices and software that commonly arrive with default, blank or weak security settings include routers, switches, wireless access points, shopping carts, point-of-sale (POS) software, payment processing software, web servers and database software.

Security settings must be changed prior to deployment for production use as they can often be easily guessed and information regarding these settings is often available on the Internet. Security settings include but are not limited to user accounts, services and software configurations.

It is important to understand which settings may be unnecessary or redundant to conduct business functions. Unnecessary services found in prior breaches (where the entity did not have a business need for these functions) 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. Services or software that is not needed may be ignored rather than disabled by system administrators. As a result, related software patches that should be installed to guard against known vulnerabilities may be ignored, thereby creating an unintended means by which hackers can gain access to critical systems.

Successful exploitation of vulnerability may result in an attacker gaining partial or complete control of the infrastructure. This may occur through the introduction of malicious software or “malware” (e.g., bots, packet sniffers, viruses and trojan horses) into the system and can result in possible cardholder data theft.

### **Risk Mitigation Strategy**

In order to harden critical systems that store or have access to cardholder data, payment system participants should take the following actions:

#### PCI DSS Requirements 1 and 2

- *Check vendor manuals and Internet resources for default, blank and weak security settings for all devices and software, and immediately change the settings upon installation. This includes changing all passwords to a unique strong password, disabling unnecessary users, and changing default usernames to custom names, as appropriate.*
- *Configure systems in accordance with the PCI DSS requirements including patch management, password management and overall security configuration.*
- *Completely disable or remove unused, redundant, and unnecessary services and software from all systems.*
- *Activate necessary security functions for all devices and software.*

## PCI DSS Requirements 6 and 7

- *Maintain the latest security patches for all systems, services and software.*
- *All system user management controls must be compliant with the PCI DSS requirements.*
- *Implement least privilege necessary for system, services and software accounts.*

## PCI DSS Requirements 8, 10 and 12

- *Determine if remote management of systems is required and disable connectivity and services where not needed.*
- *When remote access is necessary, use the latest remote access software version and implement the security features according to the vendor's instructions. For example:*
  - Ensure and regularly monitor those employees and vendors who need remote access and ensure that this access is absolutely necessary.
  - Activate remote access only when needed; immediately deactivate remote access after a specific period of inactivity and after each use.
  - Immediately change default, blank and weak settings in the remote access software to strong security settings.
  - Allow connections only from specific and known Internet Protocol (IP)/Media Access Control (MAC) addresses.
  - Use two-factor authentication (e.g., tokens, certificates or smart cards) for all employees and vendors that need remote access.
  - Use strong authentication or complex passwords for logins.
  - Enable and enforce encrypted data transmission.
  - Enable account lockout after a certain number of failed login attempts.
  - Configure systems so that a remote user must establish a VPN connection before access is permitted.
  - Ensure that the logging function is enabled for all actions including invalid login attempts.
- *Access requests to the network and connected systems should be logged to identify unusual activity and the extent of possible exposure in a suspected data compromise.*
- *Ensure that POS software or payment processing software has been validated as compliant with the PCI Payment Application Data Security Standard (PA-DSS), formerly known as Visa's Payment Application Best Practices (PABP). A list of PABP-validated applications is available at [www.visa.com/cisp](http://www.visa.com/cisp) and a list of PA-DSS validated applications is available at [www.pcisecurity-standards.org/security\\_standards/vpa](http://www.pcisecurity-standards.org/security_standards/vpa).*



### **3. Malicious Software (Malware) That Captures Cardholder Data**

Malware is designed to damage or infiltrate computer systems and includes packet sniffers, key loggers and memory dumpers that are installed on systems with access to cardholder data. While these forms of malware have legitimate IT uses for security monitoring, system and software debugging, and troubleshooting, recent compromises illustrate that attackers utilize these technologies to obtain payment card data.

Recent investigations have uncovered evidence of sniffer malware being used by network intruders to capture payment card data as it is transmitted through a compromised entity's systems and network, often during authorization of a payment card transaction. Once network intruders gain entry into an entity's systems, malware is installed and can be difficult to detect. Sniffer malware often has the capability to search specifically for cardholder data and write the data to a file so it can later be collected by the intruder. In addition to capturing cardholder data, intruders have also successfully "sniffed" or "logged" usernames and passwords of privileged accounts that allow them to take control of critical systems.

#### **Risk Mitigation Strategy**

The following essential security practices should be utilized to mitigate the risk of exposure to critical systems through malware:

#### PCI DSS Requirements 1, 3 and 4

- *Prevent cardholder data from unknowingly leaving the network.*
- *Utilize an automated tool or process to regularly scan across all systems and connected networks to locate stored cardholder data that was unintended, unauthorized or unprotected.*
- *Utilize encrypted protocols or encryption to protect cardholder data.*

#### PCI DSS Requirements 5, 6 and 7

- *Ensure that anti-virus, anti-malware and anti-spyware software programs are up-to-date.*
- *Use outside resources to help identify new security vulnerabilities. Visa provides a frequently updated data security alert that lists malware and IP addresses identified in forensic investigations, available at [www.visa.com/cisp](http://www.visa.com/cisp).*
- *Secure workstations to prevent illegitimate packet sniffers, key loggers, memory dumpers or other malware from being installed.*

#### PCI DSS Requirements 9, 10, 11 and 12

- *Routinely examine systems and networks for unknown and unauthorized debugging software and newly added hardware devices.*
- *Monitor firewalls and logs for suspicious traffic and activities, particularly outbound traffic to unknown addresses.*
- *Utilize host-based Intrusion Detection Systems (IDS).*
- *Implement file integrity monitoring.*
- *Use packet sniffers legitimately to detect network intrusion attempts or suspicious activity on a network.*

#### **4. Insecure Network Configuration and Poor Monitoring**

Securing the network and monitoring network traffic for unauthorized access is the foundation of a secure environment. The network is often a key target for security breaches and is the main vehicle for transmission of malicious software between systems.

If an intruder breaches the outside perimeter of a network, the systems within that network are at high risk of being compromised. Proper firewall rules configuration and management of network devices is critical to preventing unauthorized access. To minimize this threat, it is essential that internal networks and devices are properly managed and are not susceptible to known vulnerabilities.

Poor firewall rules configuration, network segmentation and management of network devices can expose sensitive systems to non-trusted networks and expose the network and any connected networks to malicious code and viruses, including the Internet. These types of exposures allow criminals unauthorized access, enabling them to transmit cardholder data and other sensitive data outside of the network.

#### **Risk Mitigation Strategy**

To prevent the misconfiguration of network devices, payment system participants are encouraged to adopt the following essential security practices:

##### PCI DSS Requirements 1 and 2

- *Permit inbound and outbound network traffic only where there is a defined business need; deny all other network traffic.*
- *Identify all systems that store, process or transmit cardholder data. Define separate network security zones to include systems that handle data of similar risk levels, such as cardholder data.*
- *Identify normal data flows for cardholder information into and out of the network.*
- *Configure firewall rules to deny all inbound traffic from non-trusted external networks to protected networks and systems. Larger networks should implement internal proxy servers for web traffic. This will consolidate all World Wide Web (WWW) traffic (i.e., HTTP, typically port 80, and HTTPS, typically port 443) outbound to the Internet through one server and allow for less complex firewall rules. This practice also allows for inspection of outbound WWW traffic to detect malicious activity and the possible leakage of cardholder data.*
- *System administrators should block direct remote connectivity to any databases on the firewall (e.g., for Microsoft SQL Server, typically TCP port 1433, UDP port 1434, etc.). To reduce the risk of unauthorized access, consider limiting or blocking all non-console administrative connectivity to the database on the internal network as well.*

##### PCI DSS Requirement 10

- *System Administrators should monitor the firewall and other network devices for abnormal outbound traffic, which may be associated with malicious activity. Common signs of abnormal network traffic include:*

- WWW traffic over TCP port 80 from unexpected locations on an internal, protected network such as a POS system, back-office store controller or other systems that do not normally require WWW connections.
- Internet Relay Chat (IRC) traffic over TCP port 6667 to unknown IP addresses on the Internet.
- Large volumes of data transmitted to non-trusted destinations that are not defined destinations in the outbound firewall rules.

## **5. Lack of Audit Trail Logs**

The ability to track and monitor user activities is crucial to an organization's ability to detect a system intrusion. The presence of network, system and software audit trail logs allows security personnel to review anomalous activity, identify suspicious events and respond appropriately to mitigate the compromise of cardholder data. Over a period of time, such logs can assist security personnel in establishing operational norms and developing criteria to categorize threat responses to anomalous activity. Additionally, forensic investigators utilize audit trail logs to thoroughly track and analyze suspicious activity and confirm intrusions.

Without sufficient audit trails, diligent monitoring of logs, and swift response to incidents, a breach of critical systems can remain undetected for extended periods of time. Identifying security breaches in a timely manner can mitigate the impact and potential loss of data. Determining the source and timeline of a data compromise is more difficult, or in some cases impossible, without proper audit logs.

### **Risk Mitigation Strategy**

To ensure that audit trail logs are enabled and are being monitored, payment system participants should follow these industry best practices:

#### **PCI DSS Requirement 10**

- *Enable audit trail logging for all events (including access to cardholder data and across network resources) in accordance with PCI DSS requirements, to include user ID, type of event, date and time, success or failure indication, origination of event and identity of the system component.*
- *Secure audit trail logs to prevent intruders from editing or deleting log files to conceal unauthorized or attempted access.*
  - Limit access only to those with a job-related need.
  - Monitor for both unauthorized and attempted access.
  - Protect audit trail files from unauthorized modifications.
  - Segregate logged data to an independent server.
  - Use file integrity monitoring change detection software to ensure that existing log data cannot be changed without generating alerts.
- *Utilize log management solutions that provide a scalable and centralized process to collect, normalize, aggregate, compress and encrypt log data from disparate sources.*

- Log sources may include but should not be limited to routers, switches, firewalls, intrusion detection and prevention systems, POS and payment processing software, anti-virus/anti-spam/anti-malware, Windows systems, Unix and Linux systems.
  - Solutions should automate the ability to produce reports containing relevant information that will indicate an anomaly or glitch.
- 
- *Review audit trail logs for all system components at least daily.*

## **Summary**

Payment system participants must secure their cardholder environments and immediately address these and other vulnerabilities that can lead to a breach of the network or sensitive systems. The risk of a compromise can be mitigated by achieving and maintaining PCI DSS compliance at all times while carefully addressing these five commonly exploited vulnerabilities.

Additionally, payment system participants must fully understand where cardholder data is being stored, processed or transmitted within their environments including connected non-payment systems and networks. This thorough identification is a necessary and important first step in addressing the risk of a data compromise. Further, entities must not store prohibited cardholder data (i.e., full magnetic-stripe, CVV2 or PIN data) post authorization, which is in direct violation of Visa rules and the PCI DSS. Although not required by Visa, payment system participants may retain specific cardholder data elements that support their business functions for card acceptance. Specifically, cardholder data elements that can be stored in accordance with PCI DSS are the primary account number (PAN), expiration date, name and service code.

In the event of a security incident, Visa clients must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa and report investigation findings. Additionally, entities that suspect a security breach may have occurred should contact law enforcement and consult with their legal department regarding state and federal notification laws. For additional steps to take if a compromise is suspected, please refer to the What To Do If Compromised document available at [www.visa.com/cisp](http://www.visa.com/cisp).

The protection of cardholder account information is a responsibility shared by all participants in the Visa payment system. Visa is committed to providing educational information to its key stakeholders about potential vulnerabilities and urges financial institution clients to share this information with their merchants, agents and other stakeholders

If you have any questions regarding this bulletin, please contact your Relationship Manager..