Payment Card Industry (PCI) Data Security Standard

Technical and Operational Requirements for Approved Scanning Vendors (ASVs)

Version 1.1

Release: September 2006

Table of Contents

1 PCI Security Scanning Vendor Program

This chapter provides an overview of the Payment Card Industry (PCI) Security Scanning Vendor Program.

Introduction

The Payment Card Industry has adopted a single set of requirements for cardholder data protection across the entire industry, the PCI Data Security Standard (DSS).

To validate compliance with the PCI DSS, a merchant, service provider, and/or financial institution may be required to undergo a PCI Security Scan conducted by an Approved Scanning Vendor (ASV). This document provides guidance and requirements applicable to ASVs in the framework of the PCI DSS and associated payment brand data protection programs.

Security scanning companies interested in providing scan services in conjunction with the PCI program must comply with the requirements set forth in this document and must successfully complete the PCI Security Scanning Vendor Testing and Approval Process.

Naming Convention

The following terms are used throughout this document.

Term	Definition
ASV	Approved Scanning Vendor. Data security firm using a scanning solution to determine PCI compliance of their customers
Customer	Merchant, Service Provider, or other entity that is undergoing a PCI scan
Component	Any physical or virtual device residing on the customer network
Service Providers	Third party processors, payment gateways, and other organizations that store, transmit, or process payment card information on behalf of financial institutions, payment brands, or merchants

Term	Definition
Scanning solution	Set of security services and tool(s) offered by an ASV to validate compliance of a merchant or service provider with the PCI DSS. The scanning solution includes the scanning procedures, the scanning tool(s), the associated scanning report, and the process for exchanging information between the scanning vendor and the customer

Scanning Procedures for Merchants and Service Providers

To be considered compliant with the PCI DSS validation requirement, the merchant's/service provider's infrastructure must be tested in accordance with the *Payment Card Industry (PCI) Security Scanning Procedures* document.

2 Scanning Solution Requirements

This chapter identifies the general and technical requirements for ASV scanning services.

General Requirements for Scanning Solutions

This chapter outlines generic functional requirements. ASVs **must do the following**:

- Obtain from customer the list of all Internet-facing Internet Protocol (IP) addresses and/or ranges, including all network components and devices that are involved in e-commerce transactions or retail transactions that use IP to transmit data over the Internet
- If domain-based virtual hosting is employed, obtain from customer a list of all domains to be scanned
- Scan customer's IP range to identify active IP addresses and services. If active IP addresses are found that were not originally provided by the customer, the ASV must consult with the customer to determine if these IP addresses should be included
- Scan list of active IP addresses and/or domains for known vulnerabilities and configuration issues

ASVs must conduct PCI customer system scans in accordance with this document and any supplementary guidance provided in the *Payment Card Industry Security Scanning Procedures* document.

Non-disruptive Nature of the ASV Solution

ASV solutions must provide only tests that do not damage the customers' systems or data. Solutions must not cause an activity that would result in a system reboot, or interfere with or change domain name server (DNS), routing, switching, and address resolution. Root-kits or other software must not be installed unless part of the solution and pre-approved by the customer.

The following are examples of some of the tests that are **not** permitted:

- Denial of service (DoS)
- Buffer overflow exploit
- Brute-force attack resulting in a password lockout
- Excessive usage of available communication bandwidth

Fingerprinting

Fingerprinting can reduce the load on the customer environment by eliminating tests that are not relevant to the particular environment.

The ASV scanning solution must include an exhaustive fingerprinting scan on all transmission control protocol (TCP) and user datagram protocol (UDP) ports.

Platform Independence

Customer platforms are diverse. Each platform has strengths and weaknesses. The ASV solution must cover all commonly used platforms.

Accuracy

In addition to confirmed vulnerabilities, ASVs must report all occurrences of vulnerabilities that have a reasonable level of identification certainty. When the presence of a vulnerability cannot be determined with certainty, the potential vulnerability must be reported as such.

False Positives Management

The customer may point out to the ASV that vulnerabilities identified in the scanning report are false positives. **In this case, the following is required:**

- The ASV must assess the relevance of the customer statement and make a determination of adequacy. The report should be amended by the ASV as necessary
- The customer must not be permitted to edit the scanning report
- The ASV scan must not reduce the search space of any scan by discarding any previously reported false positives

Load Balancer

The ASV should obtain written assurance from the customer that the infrastructure behind the load balancers is synchronized in terms of configuration. The configuration and the customer's assurance must be clearly documented in the scan report.

If the ASV cannot obtain customer assurance, the components must be individually scanned from an internal location (behind the load balancers).

Intrusion Detection System/Intrusion Prevention System

Under no circumstance should an intrusion detection system/intrusion prevention system (IDS/IPS) be permitted to interfere with the results of a vulnerability assessment.

When the infrastructure contains an IDS, the following options should be considered:

- IDS/IPS should be configured to monitor and log but not to act against the originating IP address of the ASV (**This is the preferred solution)**
- ASVs should scan from a network location where the IDS/IPS can not interfere with the operation

Internet Service Provider Blocked Port

In some circumstances, a packet may not reach the customer environment during the scanning process. The absence of a meaningful reply may result in misleading report conclusions.

This situation may occur when an Internet service provider (ISP) used to carry traffic during the scanning procedures blocks potentially harmful packets. For example, Network basic input/output system (NetBIOS) ports of Microsoft® Windows® systems are usually blocked by ISPs.

Prior to scanning, the ASV must ensure that there is an unfiltered communication path to the customer's environment from the originating IP address of the ASV.

Obsolete environment

The ASV must report and determine as non-compliant any identified obsolete software (for example, application software or operating systems (OSs) no longer supported by the respective manufacturers. Obsolete software may expose the infrastructure to a security-related vulnerability.

Built-in Accounts

The ASV scanning solution used for testing and reporting on built-in or default accounts in routers, firewalls, OS web servers, relational database management system (RDBMS) servers, applications, or other components, **must do the following**:

- Not use a brute-force attack or dictionary attack, but rather concentrate on known built-in or default accounts
- Report on services that are available without authentication

Sanity Check

The ASV scanning solution must be able to detect and report any backdoor applications installed on the servers.

Secure Sockets Layer/Transport Layer Security

The ASV scanning solution must be able to test for the presence of secure sockets layer (SSL)/transport layer security (TLS). The ASV scanning solution must be able to check for the SSL version, certificate validity, authenticity, and matching server name.

Technical Requirements for Scanning Solutions

The remainder of this chapter outlines the technical specifications for ASV scanning solutions.

Scope of the Assessment

Following is a non-exhaustive list of services, devices, and OSs that must be tested.

Device	Type
Operating systems	AIX®, BSD variants, including FreeBSD, Open BSD, NetBSD, Linux, Sun Solaris™, Microsoft® Windows®
Web servers	Leading web servers including Apache, Lotus® Domino, Microsoft® IIS, Sun One™
Web application servers	Leading web application servers including BEA Weblogic Server®, IBM Websphere®, Apache Jakarta Tomcat, JBOSS
Common web scripts	Commonly found scripts (typically, common gateway interface [CGI] scripts) written in various languages, particularly e-commerce related scripts (for example, shopping carts and CRM scripts), ASP, PHP
Database servers	Leading database servers including IBM DB2®, Microsoft SQL Server™, MySQL®, Oracle®, PostreSQL, Sybase®
Mail servers	Leading mail servers including Lotus® Domino, Microsoft® Exchange, Netscape® Messaging Server, SendMail™
Firewalls	Leading firewalls including Check Point®, Cisco PIX®, Gauntlet, Linux IP chains/tables, NetScreen, Raptor
Routers	Leading routers, including Cisco
Wireless access points	Leading wireless access points including Cisco, LinkSys®, NETGEAR®, Apple®, Intel®, ORiNOCO, 3Com®

Device	Type
Common services	Other common services including domain name system (DNS), file transfer protocol (FTP), simple mail transfer protocol (SMTP)
Custom web applications	Web applications must be tested for SQL injection and cross-site scripting vulnerabilities.

Router Check

The ASV scanning solution must be able to test the router for known vulnerabilities and configuration issues in the firmware.

Firewall Check

Firewall products have known vulnerabilities for which patches are released periodically. The ASV scanning solution must be able to to test if the firewall is adequately patched.

A common firewall problem is inadequate configuration. The ASV scanning solution must be able to detect and report open ports.

OS Check

New exploits are discovered routinely for OSs and security patches are released for these flaws. The ASV scanning solution must be able to verify that the OS is patched for these known exploits.

Database Check

The ASV scanning solution must be able to detect open access to databases. A database can be made to be accessible over the Internet; however, this practice is generally not considered good practice and does not comply with the PCI DSS.

New exploits are regularly found for database products. The ASV scanning solution must be able to detect these exploits.

Web Server Check

The ASV scanning solution must be able to test for all known vulnerabilities and configuration issues on web servers. New exploits are routinely discovered in web server products. The ASV scanning solution must be able to detect and report known exploits.

Browsing of directories on a web server is not a good practice. The ASV scanning solution must be able to scan the web site and verify that directory browsing is not possible on the server.

The ASV scanning solution must be able to detect all known CGI vulnerabilities.

Application Server Check

The ASV scanning solution must be able to detect the presence of an application server and detect any known vulnerability and configuration issues.

DNS Server Check

The ASV scanning solution must be able to detect the presence of a DNS server and detect any known vulnerability and configuration issues.

Mail Server Check

The ASV scanning solution must be able to detect the presence of a mail server and detect any known vulnerability and configuration issues.

Other Application Check

The ASV scanning solution must be able to detect the presence of other applications and to detect any known vulnerability and configuration issues.

Custom Web Application Check

The ASV scanning solution must be able to detect the following application vulnerabilities and configuration issues:

- Unvalidated parameters which lead to SQL injection attacks
- Cross-site scripting (XSS) flaws

Wireless Access Point Check

Wireless local area networks (WLANs) introduce new information security risks to those companies that deploy them. The ASV scanning solution should be designed to detect known vulnerabilities and configuration issues of WLAN access points if visible from the Internet.

3 Scan Report Requirements

This chapter identifies the functional requirements for the scan report.

Scan Report Requirements

After conducting a scan, the ASV produces a report with findings and recommendations. The report must assess compliance with the PCI scanning requirement at the following two levels:

1. Each scanned component
2. The global customer infrastructure

ASVs must produce reports that meet all the requirements in this section.

Report Levels

Each scanning report must include the following separate documents:

- An executive summary with compliance statement and ASV information
- Detailed findings and recommendations

Delivery

- Reports must be available either by download or e-mail in PDF format
- Reports must be delivered securely

Report integrity

ASVs must be able to verify the integrity of any copies of the report, after they have been distributed.

Report Content

The **high-level report** must include the following:

- Table of contents
- The following statement:

> "This report was generated by a PCI Approved Scanning Vendor, [insert *scanning vendor name*], under certificate number [insert *certificate number*], within the guidelines of the PCI data security initiative."

- Recommendation for meeting the scan validation requirement, based on the content of the scan report. To clearly achieve this requirement, the first sentence of the executive summary must contain the following sentence:

  > "[ASV *Name*] has determined that [*Merchant Name/ Service Provider Name*] is [*COMPLIANT* or *NOT COMPLIANT*] with the PCI scan validation requirement."

- Table with a list of each scanned IP address and corresponding compliance status (see "Component and Customer Compliance")
- Description of the severity level system used by the ASV (to prioritize solutions associated to vulnerabilities and mis-configurations)
- Date when scan was conducted and report was generated

The **detailed report** must be readable and accurate, and must include the following:

- Table of contents
- Vulnerabilities sorted by IP address and severity, with the most critical vulnerabilities listed first
- Detailed statement for each vulnerability found on the customer infrastructure, including:
  - Name
  - Industry reference numbers such as CVE, CAN, or Bugtraq ID
  - Severity level
  - Common Vulnerability Scoring System (CVSS), http://www.first.org/cvss/, base score, as indicated in the National Vulnerability Database (NVD), http://nvd.nist.gov/cvss.cfm (where available)
  - Comprehensive explanation
  - Solution or mitigation
  - References to the companies/organizations that provide the solution for the vulnerability (if available)
- For each IP address, a consolidated solution/mitigation plan

4 Component and customer compliance

This chapter identifies criteria to categorize vulnerabilities' severity and provides guidance for compliance determination.

Vulnerability Categorization and Compliance Determination

ASVs may have a unique method of reporting vulnerabilities; however, high-level risks must be reported consistently to ensure a fair and consistent compliance rating.

Table 1 contains examples of how an approved scanning solution may be configured to categorize vulnerabilities and assign severity levels. The Table demonstrates the types of vulnerabilities and risks considered at each level of severity.

If the vendor severity levels are different from the five levels described in Table 1, the vendor security levels should be mapped against these PCI levels.

To be considered compliant, a component must not contain vulnerabilities assigned Level 3, 4, or 5. To be considered compliant, all components within the customer infrastructure must be compliant. The scan report must not include any vulnerabilities that indicate features or configurations that may violate PCI DSS requirements. If vulnerabilities are detected, the ASV must consult with the client to determine if these are, in fact, PCI DSS violations and warrant a noncompliant scan report.

The scan report must reference all vulnerabilities discovered. If a merchant or service provider identifies any vulnerability as a false positive or is unable to remediate any vulnerability due to technical constraints, but acceptable compensating controls exist, the ASV must contact the client to determine, if possible, the validity of the claim. The ASV must document these findings in the scan report.

Level	Severity	Description
5	**Urgent**	Trojan Horses; file read and writes exploit; remote command execution
4	**Critical**	Potential Trojan Horses; file read exploit
3	**High**	Limited exploit of read; directory browsing; DoS
2	**Medium**	Sensitive configuration information can be obtained by hackers
1	**Low**	Information can be obtained by hackers on configuration

Table 1 Vulnerability Severity Levels

Level 5

Level 5 vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers full file-system read and write capabilities, and remote execution of commands as a root or administrator user. The presence of backdoors and Trojans qualify as Level 5 vulnerabilities.

Level 4

Level 4 vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities. Level 4 vulnerabilities give hackers partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information qualify as Level 4 vulnerabilities.

Level 3

Level 3 vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of vulnerabilities could result in potential misuse of the host by intruders. Examples of Level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to DoS attacks, and unauthorized use of services such as mail relaying.

Level 2

Level 2 vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks against a host.

Level 1

Level 1 vulnerabilities expose information such as open ports.

New Vulnerability Categorization and Compliance Determination Requirements

Effective June 30, 2007, ASVs must determine compliance based on the following new requirements.

Vulnerability categorization

To assist customers in prioritizing the solution or mitigation of identified issues, ASVs must assign a severity level to each identified vulnerability or mis-configuration.

The designation of each severity level must allow an easy comparison between levels. Therefore, a severity ranking that is easy to understand must be presented, such as with levels Low Priority, Medium Priority, and Urgent.

Wherever possible, the ASV must use the CVSS base score for the severity level.

Compliance determination

Reports must indicate compliance determination at two levels: component and (global) customer level.

The following statements provide the necessary guidance to ASVs to determine compliance at component level and customer level.

Component compliance determination

Generally, to be considered compliant, a component must not contain any vulnerability that has been assigned a CVSS base score equal to or higher than 4.0.

If a CVSS base score is not available for a given vulnerability identified in the component, then the compliance criteria to be used by the ASV is the possibility of the identified vulnerability leading to a data compromise.

The following exceptions or clarifications apply:

- A component must be considered non-compliant if the installed SSL version is limited to Version 2.0, or older. SSL must be a more recent version than 2.0.
- Vulnerabilities or mis-configurations that may lead to DoS should not be taken into consideration by the ASV when determining component compliance

- The presence of application vulnerabilities on a component that may lead to SQL injection attacks and cross-site scripting flaws must result in a non-compliant status for that component

Global compliance determination

For a customer to be considered compliant, all components within the customer's cardholder data environment must be compliant. The cardholder data environment includes the entire network infrastructure unless physical or logical network segmentation is in place.