PCI DSS 合规建设 ASV 扫描介绍

atsec 信息安全 陈谨运

关键词：PCI、渗透测试、支付卡行业、atsec 、安全评估、ASV 、授权扫描商

atsec(Beijing) information technology Co., Ltd

Room 119, Building 2, No.1, Street 7, Shangdi,

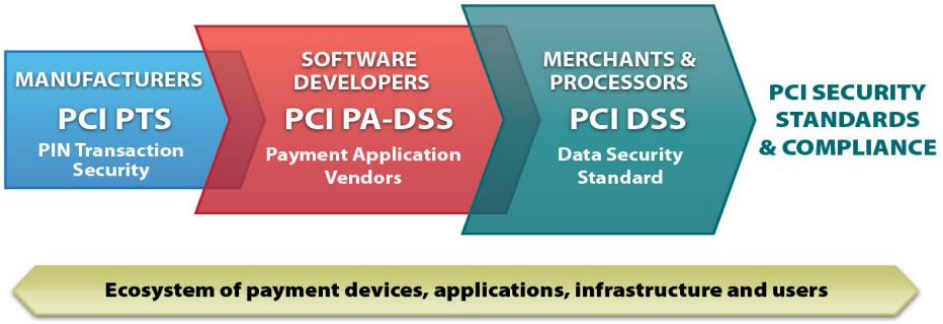
Haidian District, Beijing, P.R.China 10085

Tel +86-10-84834011

Fax +86-10-82890017

PCI DSS 介绍

PCI（Payment Card Industry）中文全称为：支付卡产业。在这个产业里存在一个标准组织，称为--支付卡行业安全标准委员会，英文简写为 PCI SSC（Payment Card Industry Security Standards Council）。PCI 安全标准委员会是由国际知名的五家支付品牌共同建立而成，他们是美国运通（American Express）、美国发现金融服务公司（Discover Financial Services）、JCB、全球万事达卡组织（MasterCard）及 Visa 国际组织。PCI SSC 一共维护了三个安全标准：PCI DSS（Payment Card Industry Data Security Standard 支付卡行业数据安全标准）、PCI PA-DSS（Payment Card Industry Payments Application Data Security Standard 支付卡行业支付应用数据安全标准）以及 PTS（PIN Transaction Security PIN 传输安全标准）。从下图可以很清楚的反应这三个标准之间的关系。



无论是 PTS 还是 PCI PA DSS，其最根本的目的是为了使最终的客户能够满足 PCI DSS 的要求。（关于 PTS 和 PA DSS 更多的介绍可参见 PCI 官方网站 www.pcisecuritystandards.org 和 atsec 官方网站 www.atsec-information-security.cn）。

在PCI DSS第 11.2.2中有这样的要求“Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).”其转译中文意思是：每季度由PCI SSC认可的授权扫描服务商(Approved Scanning Vendor) --- ASV执行外部的脆弱性扫描。

什么是 ASVs

授权扫描服务商是经过 PCI SSC 认可的，为商户和服务提供商的对外提供服务的互联网环境执行脆弱性扫描的组织，它的目的是为了验证商户和服务提供商遵守一定的 PCI DSS 要求（PCI DSS 11.2 要求）。

PCI DSS 对于 ASVs 的要求

对于ASVs而言，PCI SSC维护了一套认证的流程，详细的认证流程可参见PCI SSC的指引文件。根据要求ASVs每年都需要进行资质的重新认证，认证的结果可以从PCI官方网站上查询到，详细地址参见：https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

对于 ASVs 的认证，PCI SSC 除了对公司的资质要求以外，扫描工具也需要经过 PCI SSC 的认可。除此以外执行 ASV 扫描的人员则需要通过 PCI SSC 的 ASV 在线考试。

ASV 扫描的流程

根据PCI SSC的规定，所有ASV的执行过程和流程都应该要满足“asv_program_guide_v1.0”的要求。

该指导文件描述了ASV扫描流程中的不同角色，扫描范围的确定，脆弱性分类，扫描报告内容描述，误报处理，报告的交付和完整性保护，质量保证等内容。

ASV 范围的确定

在执行 ASV 扫描之前，执行扫描的人员需要与客户一起去确定 ASV 扫描的范围。通常客户需要提供其对外提供服务的所有 IP 地址列表，网络拓扑图以及相关的资料以便扫描人员能够根据 PCI DSS 要求判断那些系统组件应该要在扫描的范围之内。按照 PCI DSS 的要求：所有对外提供服务的涉及持卡人信息传输，处理或者存储的系统组件都需要每季度执行 ASV 扫描。这里的系统组件包括但不限于服务器，网络设备，安全设备。

在初步确定 ASV 扫描范围之后，扫描人员需要使用 ASV 扫描工具的“探测”功能去探测目标系统以及与其相关联系统组件的状态。在这个环节当中， ASV 扫描工具会自动化的去识别与预设目标相关联的系统组件的活动状态，所以“探测”扫描发现的 IP 地址数量通常会比预设目标的 IP 数量会更多。这时候扫描人员就需要根据发现的结果与客户进行讨论以最终确认 ASV 的扫描范围。

如何判断是否通过 ASV 的扫描

对于ASV扫描的结果，很多客户都会关心什么样的条件能够通过ASV扫描，是否有统一的标准？根据PCI SSC“asv_program_guide_v1.0”的描述，所有包含高危严重级别的脆弱性和任何违反PCI DSS的功能或配置的脆弱性都将不能通过ASV的扫描。

以下是CVSS评分和NVD严重级别与ASV扫描结果的对应关系：除了少数特定情况，任何CVSS分值大于或者等于4.0的脆弱性都不能够通过ASV扫描

CVSS 分值	严重级别	ASV 扫描结果	指导
7.0 -- 10.0	高危	失败	为能够通过 ASV 扫描，这些脆弱性被修复并且在脆弱性修复之后需要再次执行扫描。组织应采取以风险级别为基础的方法来纠正这些漏洞，按照风险的危害程度最关键的（CVSS 分值为 10.0）脆弱性应当最先修复，然后修复 CVSS 分值为 9 的脆弱性，直到 CVSS 分值从 4.0 至 10.0 的所有漏洞都被纠正。
4.0 -- 6.9	中危	失败	
0.0 -- 3.9	低危	通过	CVSS 分值从 0.0 至 3.9 的脆弱性是能够通过 ASV 扫描的，但是从安全角度建议（非强制）对这些脆弱性进行修复。

对于 NVD 严重级别与 ASV 扫描结果的对应关系而言会存在一些特殊的情况，以下是需要 ASV 特殊考虑的情况：

- ☐ **该脆弱性并没有被 NVD 收录**
- ☐ **ASV 不认同在 NVD 中给出的 CVSS 分值**
- ☐ **纯粹的拒绝服务（DoS）脆弱性**
- ☐ **该脆弱性违反 PCI DSS 的要求或者风险级别高于 NVD 的描述**

ASV 扫描报告

PCI SSC 对于 ASV 扫描报告格式有严格的要求，每个 ASV 在报告中都需要包含以下的内容：

- ☐ **扫描认证的合规性**
  这部分的内容是整体的总结，主要显示客户的基础架构是否满足 PCI DSS 审核要求并且通过 ASV 的扫描。
- ☐ **ASV 扫描报告执行摘要**
  这一章节的内容需要列举组件（通过 IP 地址的形式）的脆弱性以显示每个被扫描的 IP 地址是否满足 PCI DSS 审核要求并且通过 ASV 的扫描。这个章节当中，所有的脆弱性都会对应到特定的 IP 地址，每个脆弱性都会与 IP 地址一一对应。
- ☐ **ASV 扫描报告漏洞详细资料**
  这个章节包含对应脆弱性合规的状态（通过 / 失败）的总结以及被发现的脆弱性的详细描述。

除上述描述以外，作为一份被认可的 ASV 扫描报告，它需要包含两个非常重要的元素：被扫描客户对 ASV 扫描的认可声明（包括扫描的范围，客户的信息等内容）另外一个则是具有 PCI SSC ASV 资质认定的人员对于报告的认可。其中最后一个元素被视为 ASV 扫描报告有效性的证明。任何没有经由具有 PCI SSC ASV 资质认定的人员声明的 ASV 报告将不被视为一份合规的 ASV 扫描报告。

参考文档和链接

[1] PCI DSS https://www.pcisecuritystandards.org/security_standards/index.php

[2] ASV Program Guide v1.0
https://www.pcisecuritystandards.org/documents/asv_program_guide_v1.0.pdf

[3] QualysGuard www.qualys.com/products

[4] CVE http://cve.mitre.org/

[5] CVSS http://www.first.org/cvss/