补充信息

从 SSL 和早期 TLS 迁移

1.1 版
日期：2016 年 4 月
著作方：PCI 安全标准协会

实施概要

到该迁移的时刻了。

自发布以来的 20 多年间，安全套接层 (SSL) 一直是市场上最广泛应用的加密协议之一，而且至今仍普遍使用（虽然该协议具有多个安全漏洞）。

SSL v3.0 于 1999 年由 TLS v1.0 取代，该协议之后又为 TLS v1.1 和 v1.2 所取代。如今，SSL 和早期 TLS 因为存在无补丁修复的安全漏洞，而不再符合最低安全标准。对实体而言至关重要的是尽快升级至安全协议，并停用任何对 SSL 和早期 TLS 的降级。

在 PCI DSS v3.1（2015 年 4 月版）中，SSL/早期 TLS 从强效加密法示例中移除。

具有哪些风险？

SSL/TLS 对两个端点之间（例如，网络浏览器和网络服务器之间）的渠道进行加密，从而为通过该通信渠道传输的数据确保保密性和可靠性。自 SSL v3.0 发布以来，已发现多个漏洞，开发人员在 2014 年末发布了最新安全漏洞 (CVE-2014-3566) 的相关详情，攻击者可能可利用此漏洞来从安全连接提取数据。此漏洞更常称为 POODLE（Padding Oracle 降级旧版加密），属于中间人攻击，可能可对 SSL v3.0 保障的加密讯息进行解密。

SSL 协议（所有版本）无法修复；尚无已知方法来补救 POODLE 等漏洞。SSL 和早期 TLS 不再符合实体对于实施强效加密法来保护公共或未受信任通信渠道所传输支付数据的安全需求。而且，现代网络浏览器已开始禁止 SSL 连接，以防止浏览器用户访问尚未迁移至更现代化协议的网络服务器。

应如何应对？

最佳应对方法是完全停用 SSL 并迁移至更现代化的加密协议（在本文发布时为 TLS v1.1 或更高版本），但强烈建议实体考虑 TLS v1.2。请注意，并非所有 TLS v1.1 实施都视为安全，有关安全 TLS 配置的指导，请参见 NIST SP 800-52 版本 1。

对于 PCI DSS 的影响

按照 PCI DSS v3.1，SSL 和早期 TLS 不再属于强效加密法或安全协议。直接受影响的 PCI DSS 要求有：

要求 2.2.3 针对任何被视为不安全的必要服务、协议或守护进程实施附加安全功能。

要求 2.3 使用强效加密法对所有非控制台管理访问进行加密。

要求 4.1 使用强效加密法和安全协议来保护经由公开、公共网络传输的敏感持卡人数据。

不得将 SSL 和早期 TLS 用作用于满足上述要求的安全控制。为支持致力于从 SSL/早期 TLS 迁移的实体，包含了以下规定：

- 新实施项目不得将 SSL 或早期 TLS 用作安全控制（有关新实施和现有实施的指导，参见下一节）。
- 所有服务提供商均须在 **2016** 年 6 月 30 日前提供安全 TLS 服务产品
- **2018** 年 6 月 30 日后，所有实体均须已停止将 SSL/早期 TLS 用作安全控制，并且仅使用协议的安全版本（下文最后一个要点对特定 POS POI 终端许可进行了说明）。
- 2018 年 6 月 30 日前，使用 SSL 和/或早期 TLS 的现有实施项目须采用正式的风险降低和迁移计划。
- 可被确认为不易受任何已知 SSL 和早期 TLS 漏洞影响的 POS POI 终端（及其连接到的 SSL/TLS 终端点）可在 2018 年 6 月 30 日后继续用作安全控制。

如果使用 SSL/早期 TLS，则适用 PCI DSS 附件 A2“*针对使用 SSL/早期 TLS 的实体的 PCI DSS 附加要求*”。

了解“新”和“现有”实施

当前未依赖使用易受攻击协议的实施视为“新实施”。视为“新”实施的情况示例包括：

- 为目前仅使用安全协议的环境安装系统
- 为目前仅使用安全协议的环境安装应用程序
- 构建新系统或网络来与其他支持安全协议的系统/网络通信

如果新实施无需支持已有易受攻击协议使用，则必须仅采用安全协议和强效加密法，并配置为不允许降级至易受攻击的协议。

注：*新的电子商务实施不得将消费者网络浏览器考虑为需要支持的已有基础架构。*

相反，“现有”实施为已有易受攻击协议依赖或使用的实施。视为“现有”实施的情况示例包括：

- 为目前使用和/或需要支持易受攻击协议的环境安装系统
- 为目前使用和/或需要支持易受攻击协议的环境安装应用程序
- 构建新系统或网络来与其他目前使用易受攻击协议的系统/网络通信

建议立即升级现有实施，因为继续使用 SSL/早期 TLS 可能会为电子商务环境带来风险。

准备风险降低和迁移计划

风险降低和迁移计划是一份由实体起草的文件，其中详述迁移到安全协议的计划，并说明为降低完成迁移前存在的 SSL/早期 TLS 相关风险所采用的适当控制。风险降低和迁移计划需要作为 PCI DSS 评估流程的一部分提供给评估人员。

下面提供了有关风险降低和迁移计划中应记录信息的指导和示例：

- 有关如何使用易受攻击协议的说明，包括：
  - 所用协议位于的环境类型，例如使用该协议的支付渠道类型和功能
  - 所传输的数据类型，例如支付卡帐户数据元素、管理连接等
  - 使用和/或支持该协议的系统数和类型，例如 POS POI 终端、支付交换机等
- 风险评估结果和适当的风险降低控制：
  - 实体应已评估和记录其环境风险，并实施风险降低控制措施来帮助在完全移除易受攻击协议前降低该风险。
- 有关已实施以用于监控易受攻击协议相关新漏洞的流程的说明：
  - 实体需要积极主动地时刻留意新漏洞动态。如有新漏洞发布，实体需要评估此类漏洞对其环境的风险，并确定是否需要在完成迁移前实施其他风险降低控制。
- 有关已实施以用于确保未在新环境中实施 SSL/早期 TLS 的变更控制流程的说明：
  - 如果实体目前未使用或无需支持易受攻击的协议，则完全不必为其环境引入此类协议。变更控制流程包括评估变更影响，以确认变更不会为环境带来新的安全问题。
- 迁移项目计划概览包括目标迁移完成日期（不迟于 2018 年 6 月 30 日）：
  - 迁移计划文件应标识所迁移的系统/环境和迁移时间，以及总体迁移完成的目标日期。总体迁移完成的目标日期不得迟于 2018 年 6 月 30 日。

FAQ（常见问题）

什么是风险降低控制？

对于目前使用易受攻击协议的环境，实施和持续使用风险降低控制可帮助在完全迁移至安全环境前保护易受攻击的环境。

可帮助降低风险的控制措施包括但不限于：

- 将使用易受攻击协议的功能整合到更少系统并减少支持此类协议的系统数，从而尽可能缩小受攻击面。
- 移除或停用不必要的网络浏览器、JavaScript 和影响安全的会话 Cookie。
- 检测和封阻降级至较低版本协议的请求，以限制使用易受攻击协议的通信数。

- 限制为仅允许特定实体使用易受攻击的协议，例如将防火墙配置为仅允许 SSL/早期 TLS 用于已知 IP 地址（例如，要求使用此类协议的业务合作伙伴），并封阻针对其他所有 IP 地址的此类流量。
- 扩展防入侵保护系统的覆盖区域、更新签名并封阻表示恶意行为的网络活动，以增强检测/防御能力。
- 积极监控可疑活动（例如，识别有关降级至易受攻击协议的请求数异常增多）并作出适当应对。

此外，实体应确保所有适用 PCI DSS 要求也均满足，包括：

- 积极主动地留意新漏洞动态，例如订阅漏洞通知服务和供应商支持网站，以在新漏洞出现时接收相关更新。
- 遵循供应商建议以安全配置其技术。

具有哪些迁移选项？

可实施并用作安全控制以替代 SSL/早期 TLS 的其他加密法可能包括：

- 升级至安全实施并配置为不接受降级至 SSL/早期 TLS 的最新安全版本 TLS。
- 在通过 SSL/早期 TLS 发送前，通过强效加密法加密数据（例如，使用现场级或应用程序级加密法来在传输前加密数据）
- 先设置强效加密的会话（例如 IPSEC 渠道），然后在安全渠道内通过 SSL 发送数据

而且，双因素验证可与上述控制方法组合使用，以提供验证保证。

选择的替代加密控制方法将基于特殊环境的技术和业务需求。

对于小型商户环境如何？

所有类型的实体都受到 SSL/早期 TLS 问题影响，包括小型商户。因此至关重要的是，小型商户必须采取必要措施来从其持卡人数据环境中移除 SSL/早期 TLS，以确保客户数据安全无忧。

对于 POI 环境，建议小型商户联系其终端提供商和/或收单机构（商业银行），以确定其 POS POI 终端是否受 SSL 漏洞影响。

对于其他环境（例如虚拟支付终端、后台服务器、用户计算机等），小型商户应确认是否使用 SSL/早期 TLS 及其实施位置（如果使用），然后确定能否立即执行升级，或是否存在需要延迟升级（不迟于 2018 年 6 月 30 日）的业务理由。

针对您环境的考虑事项建议包括：

- 查看您系统所使用的网络浏览器版本，由于旧版本使用 SSL/早期 TLS，您可能需要升级至新版本的浏览器
- 查看防火墙配置，以确认能否封阻 SSL
- 查看所有应用程序和系统补丁是否为最新版本
- 检查和监控系统，以识别可能表示安全问题的可疑活动

而且，在计划迁移到安全环境时，您必须制定风险降低和迁移计划。

商户应如何处理支持 SSL/早期 TLS 的 POI 终端？

当事实表明 POI 不易受当前已知漏洞影响时，POI 便可继续使用 SSL/早期 TLS。然而， SSL 是一项过时的技术，并且可能受未来其他安全漏洞的影响；因此，强烈建议尽可能为 POI 环境使用 TLS v1.1 或更高版本。新的 POI 实施应重点考虑支持和使用 TLS 1.2 或更高版本。如果环境不需要 SSL/早期 TLS，则应禁用使用和退回到这些版本。

在审核使用 SSL/早期 TLS 的 POI 终端实施时，评估人员应审查支持文件（例如，POI 供应商提供的文件、系统/网络配置详情等），以确定该实施是否易受已知利用影响。

如果 POS POI 环境易受已知漏洞的影响，则应立即着手制定迁移到安全备选方案的计划。

注：根据当前已知风险许可当前不易受漏洞影响的 POS POI。如果为易受影响的 POI 环境引入了新的漏洞，则需更新 POI 环境。

为什么 POS POI 环境更易受攻击？

PCI DSS 使 SSL 和早期 TLS 能够继续用于销售点 (POS) 交互点 (POI) 设备及其终端点。这是因为本文发布时已知的漏洞在此类环境中一般更难利用。

例如：攻击者利用一些当前 SSL 漏洞来拦截客户端/服务器通信，并操纵发送至客户端的讯息。攻击者的目的是欺骗客户端以使其发送更多数据，以便攻击者用于对会话造成威胁。具有以下特征的 POS POI 设备一般对此类漏洞更具抵抗力：

- 此类设备不支持多个客户端连接（这会促进 POODLE 攻击）。
- 该支付协议遵循 ISO 20022（通用金融业报文架构）/ISO 8583-1:2003（金融交易卡原始报文 – 交换报文规范），或限制可通过“重放攻击”接触的数据量的同等标准。
- 此类设备不使用网络浏览器软件、JavaScript 或有关安全的会话 Cookie。

注：这些特征仅用作示例，所有实施都需要经过独立评估来确定易受漏洞影响性。

还需注意，漏洞利用情况会不断发展，因此组织必须准备好应对新威胁。所有使用 SSL/早期 TLS 的组织都应尽快计划升级至强效加密协议。

POS POI 环境中对 SSL/早期 TLS 的临时使用必须具有最新补丁，并确保仅启用必要扩展。

这对于支持 POI 环境的支付处理商有何影响？

所有类型的实体都受 SSL/早期 TLS 问题影响，包括支付处理商、支付网关和其他提供交易处理服务的实体。这些实体将需要像其他实体一样，审查其 SSL/早期 TLS 使用状况，并制定迁移计划。

具有 POI 终端点的支付处理实体将需要确认如果继续使用 SSL/早期 TLS，POI 通信不会易受攻击（参见上文“为何 POS POI 环境更易受攻击”部分）。

如果某支付处理实体在同一终端点支持多个支付渠道（例如 POI 和电子商务交易），则该实体需要确保所有易受攻击的渠道都在 2018 年 6 月 30 日前迁移至安全环境。如果 POI 环境视为不易受漏洞影响，实体可能需要考虑以下选项：

- 将 POI 渠道迁移到安全环境，以便 POI 和电子商务交易可继续使用同一终端点。
- 如果不迁移 POI 渠道，可通过单独的终端点/界面来将使用 SSL/早期 TLS 的 POI 流量与已迁移至安全环境的电子商务流量分离。

对于电子商务环境如何？

由于属于基于网络的环境，电子商务实施具有最高程度的易受影响性，进而在已知 SSL/早期 TLS 漏洞方面具有即时风险。

因此，新的电子商务网站不得使用或支持 SSL/早期 TLS。

当前需要使用 SSL/早期 TLS 来支持客户的电子商务环境必须尽快开始迁移，所有此类迁移都应在 2018 年 6 月 30 日前完成。如果无法立即迁移，必须将相应理由记录成文，并加入风险降低和迁移计划。

建议在迁移完成前，尽可能减少支持 SSL/早期 TLS 的服务器数量。减少易受攻击的系统数可降低潜在利用几率，并帮助简化风险降低控制，例如增强对可疑流量的监控。

我们还鼓励电子商务商户建议其客户升级网络浏览器，以支持安全协议。

如何开始迁移流程？

下面提供了一些建议步骤，以帮助实体规划如何迁移至安全环境：

1. 识别依赖和/或支持易受攻击协议的所有系统组件和数据流
2. 对于各系统组件或数据流，识别使用易受攻击协议的业务和/或技术需求
3. 立即移除或停用所有不具支持业务或技术需求的易受攻击协议实例
4. 识别用于替代易受攻击协议的技术，并记录要实施的安全配置

5. 记录概述更新步骤和时间表的迁移项目计划
6. 实施风险降低控制来帮助在从环境移除易受攻击协议前，降低对已知利用攻击的易受影响性
7. 执行迁移并遵循变更控制程序，以确保系统更新经过测试和授权
8. 在完成新协议迁移后，更新系统配置标准

SSL/早期 TLS 能否在不用作安全控制的情况下保留在环境中？

可以，这些协议仍可在不用作安全控制的情况下，继续在系统中使用。

而且，所有在 ASV 扫描中评为 CVSS 4 或更高或者在实体内部易受攻击性扫描中评为“高”的 SSL/TLS 漏洞都必须在规定时限（例如，对于 ASV 扫描为按季度）内解决，以符合 PCI DSS 要求 11.2。按照规定的漏洞管理流程来记录如何解决 SSL/TLS 漏洞，例如仅将其用于不易受利用攻击的 POI 通信，或未移除但不用作安全控制（例如，未用于保护通信保密性）。

如果使用 SSL/早期 TLS 未产生持卡人数据威胁，是否还适用迁移日期？

是，从 SSL/早期 TLS 迁移的日期不受未来可能发生的支付卡数据威胁数影响。PCI DSS 要求旨在通过深度防御方法帮助预防持卡人数据威胁。等到潜在数据外泄公布再采取数据保护措施不仅不是有效的安全方法，而且不受 PCI DSS 支持。

使用 SSL 对 ASV 扫描结果有何影响？

SSL v3.0 和早期 TLS 包含大量漏洞，其中一些漏洞导致当前 CVSS（常见漏洞评分系统）评分为 4.3。CVSS 以 NVD（国家漏洞数据库）定义，是 ASV 必须使用的评分系统。任何中等或高风险漏洞（即 CVSS 评分 4.0 或更高的漏洞）都必须得到纠正，且相关系统必须在纠正后进行重新扫描，并表明相关问题已解决。

不过，其中一些漏洞尚无已知补救方法，建议的风险降低方法为尽快迁移至安全环境。无法立即迁移到安全环境的实体应与 ASV 合作，按照如下要求记录其特殊情况：

- *2018 年 6 月 30 日前：*未完成迁移的实体应向 ASV 提供有关其已实施风险降低和迁移计划并且正在努力按要求时限完成迁移的记录确认。ASV 应将对此确认的接收作为例外情况记录在 ASV 扫描报告执行摘要的“例外、误报或补偿性控制”下，且 ASV 可为相关扫描组件或主机签发“通过”结果（如果该主机符合所有适用的扫描要求）。
- *2018 年 6 月 30 日后：*未完全从 SSL/早期 TLS 迁移的实体需要遵循“利用补偿性控制解决漏洞”流程，来确认相关系统不易受相应特殊漏洞影响。例如，如果 SSL/早期 TLS 存在但未用作安全控制（例如，未用于保护通信保密性）。

如果实体具有已确认不易受特定漏洞影响的 POS POI 终端和/或终端点，可能可就这些系统获得 NVD 评分降低。在此类情况下，（除所有其他要求报告元素外）ASV 必须按照 ASV 计划指导提供以下信息：

- 漏洞的 NVD 评分
- ASV 的漏洞评分
- ASV 为何不认同 NVD 评分

例如，ASV 可能认为特定漏洞在特殊 POS POI 环境中的利用难度比一般 NVD 评分系统的相应定义更高。ASV 可在之后针对相关系统，为特定漏洞对评分系统的此元素进行重新排名。

进行任何此类调整时，ASV 必须考虑客户的独特环境、系统和控制，而不得基于一般趋势或假设进行此类调整。扫描客户应与其 ASV 合作，帮助了解其环境；否则 ASV 将无法确定更改 CVSS 评分是否恰当。

ASV 必须在部署此类许可时进行尽职调查和应有关注，并确保具有充足证据来支持此 CVSS 评分变更。所有此类变更都必须遵循 ASV 计划指导中规定的相应流程。

所有 ASV 扫描报告都必须按照 ASV 计划指导中规定的相应流程完成。

这是否意味着，具有风险降低和迁移计划的实体无需对 SSL/早期 TLS 中的漏洞进行补丁修复？

不，目标迁移日期不是延迟漏洞补丁修复的可接受理由。对于新威胁和风险，必须按照适用的 PCI DSS 要求（例如 6.1、6.2 和 11.2）进行持续管理，而且实体必须解决具有可用安全更新、修复或补丁的漏洞。

这对支持安全协议（例如 TLS v1.2）和非安全协议（例如 SSL/早期 TLS）的服务有何影响？

许多服务提供商（例如共享托管服务提供商）为范围广泛的各类客户提供平台和服务，其中可能包括需要和无需满足 PCI DSS 要求的实体。 支持客户 CDE 的服务提供商可表明代表客户遵循适用要求，或提供符合 PCI DSS 要求的服务选项以供客户使用。服务提供商应向其客户明确告知所提供的安全协议、如何配置不同选项，以及使用视为不安全的配置所产生的影响。

例如，网络托管服务提供商可为支持 TLS v1.2 和较弱协议的商户提供托管网络平台。为支持其客户的 PCI DSS 合规性，托管服务提供商需要为客户提供明确说明，以便其将服务使用配置为仅使用 TLS v1.2，而不降级至 SSL/早期 TLS。对于客户，在 PCI DSS 实施中使用此平台的商户需要确保所用配置选项包括 TLS v1.2，而不降级至 SSL/早期 TLS。

在混合托管环境中使用较弱协议可能会导致无法通过 ASV 扫描。在此类情况下，服务提供商和 ASV 应按照“例外、误报或补偿性控制”流程来记录如何解决相关风险，例如确认服务提供商未将 SSL/早期 TLS 用作安全控制，且提供不允许降级至较弱协议的安全配置选项以供客户使用。ASV 可为相关扫描组件或主机签发“通过”结果（如果该主机符合所有适用的扫描要求）。