商家安全

系统升级指南

要了解 SHA-256 相关合规性信息，请点击这里。

安全升级，未雨绸缪。

全球安全威胁瞬息万变，商家的安全依然是我们的首要任务。为了防范目前及将来的威胁，我们鼓励您对自己的集成执行以下升级：

1. 停止使用VeriSign G2根证书
2. 更新您的集成，使其支持使用SHA-256算法的证书

为什么要变更证书？

公共证书授权（CA）行业不断提高SSL证书的安全性。为准备在2016年要求使用SHA-256签名算法，VeriSign G2根证书将不再受支持。此证书历来被用于连接PayPal API和即时付款通知（IPN）端点。

我需要什么时候执行更新？

我们建议您尽快采取行动，为应对这些变化做好准备。

有关详细的时间表（包括在线和Sandbox API端点升级日期），请参见我们的2015-2016 SSL证书变更微站。

NOTE: 这些变更旨在解决全行业普遍存在的安全问题，并非PayPal所独有。实施更新后，它们将提高PayPal集成的隐私性和可靠性。由于这些更新细节因系统而异，我们建议在合格的系统管理员的帮助下进行更新。

1. 停止使用VeriSign G2根证书

问题：过去，VeriSign颁发的SSL证书有一个由1024位G2根证书签名的信任链。近年来，美国政府和公共CA行业已转至使用更安全的2048位证书，因此，VeriSign现在颁发的SSL证书拥有由2006年所颁发的2048位G5根证书签名的信任链。

我们的应对策略：根据行业标准，对于预期我们的证书/信任链由G2根证书签名的到API/IPN端点的安全连接，我们将不再接受。仅预期我们的证书/信任链由G5根证书签名的安全连接请求可成功实现安全连接。

您必须做什么……

如果您的系统当前授权使用VeriSign根证书，则必须停止使用依赖G2证书的SSL连接。支付行业正积极努力，计划在今年逐步淘汰 1024位根证书。

- 不支持使用G2根证书签名证书链的安全连接：

组织单位	Class 3 Public Primary Certification Authority - **G2**
序列号	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
证书SHA1指纹	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- 支持使用G5根证书签名证书链的安全连接：

通用名	VeriSign Class 3 Public Primary Certification Authority - **G5**
序列号	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
证书SHA1指纹	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

遵循这些指导原则，确保使用受支持的VeriSign G5根证书进行安全连接：

1. **检查证书存储库。**请求您的网站主机或系统管理员确认VeriSign G5根证书是否包含在您的代码用于验证逻辑的根存储库中。如果是，则无需进行任何操作。
   - 参照以下链接，检查您的密钥库中是否有使用Java、Linux或Windows的G5根证书。
2. **检查您的错误日志。**如果未下载VeriSign G5根证书来替换G2根证书，您可能会看到类似于以下内容的错误消息：
   - SSL握手错误，“No trusted certificate found”（未找到可信任的证书）
   - 结果代码-31，“The certificate chain did not validate, no local certificate found”（证书链未经验证，未找到本地证书）
   - 结果代码-8，“SSL connection failed”（SSL连接失败）
   - -1错误

   为解决这些问题，请执行以下操作之一：
   - 将您的软件更新至支持SHA-256的最新版本，或者
   - 如果使用密钥库进行证书验证/认证，请将VeriSign G5根证书安装到您的密钥库中。
3. **获得VeriSign G5根证书。**如果您的证书存储库或Java客户端不包含VeriSign G5根证书，则请您的系统管理员从VeriSign下载此根证书，然后将其保存到证书存储库和任何其他SSL连接验证包。
   - 下载Symantec的VeriSign G5根证书
   - 如果服务器要求，则下载特定服务器SSL证书

2. 更新为SHA-256签名算法

问题：SHA-1是一个已经使用了22年的密码算法，因计算能力增强而受到威胁。SHA-256将更强的算法与256位哈希值结合使用。

我们的应对策略：我们正在将所有在线和Sandbox端点上的SSL证书从SHA-1升级为更强、更可靠的SHA-256、将在2016年年中完成升级。

您必须做什么……

遵循这些指导原则，将使用SHA-1签名算法的SSL证书换成使用更强SHA-256签名算法的SSL证书：

1. **检查您的环境。**确保您的环境支持SHA-256证书。
   - 请参阅在线资源，如DigiCert的SHA-2兼容性指南和Symantec的支持浏览器和服务器列表，获取受支持的软硬件列表。
   - 如果您的部分环境不支持SHA-256，您将需要替换或升级这些部分，然后才能实施新证书。
   - Windows 2000 Server和某些版本的Windows XP可能与SHA-2不兼容。这一篇关于SHA2和Windows的Windows PKI博客可提供有关升级环境的补丁和建议。
2. **检查您的证书。**如果您的环境支持SHA-256，请确保密钥库中拥有VeriSign G5根证书。

有问题吗？

有关更多详情和常见问题，请参见我们的2015-2016 SSL证书变更微站。

谢谢您！

感谢您及时关注此问题并理解我们的做法。尽管我们承认这些步骤可能会引起兼容性问题，但比起我们共同对我们各自客户许下的确保其账户和财务信息更安全的承诺，短期内的这点不便是微不足道的。