SSL 证书部署漏洞应引起高度重视

笔者于 **2010 年 12 月 6 日**以《计算机世界》特约撰稿人的身份发表了《**网银 SSL 证书部署有漏洞**》的技术文章，指出了当时的各大银行的网银 SSL 证书部署出现的六大安全问题。并在 **2021 年 12 月 24 日**发表的博文《网银 SSL 证书部署还有漏洞？》中指出：11 年后的今天，各大银行的网银 SSL 证书安全部署情况仍然不容乐观。

今天，笔者再给第三方支付服务提供商官网、电商官网的 SSL 证书部署情况做了一次安全体检，仍然是使用 Qualys SSL 体检从 SSL 证书、协议支持、密钥交换和加密套件强度等 4 个维度来检测，体检结果也不容乐观，希望相关公司能高度重视这些安全问题，因为部署 SSL 证书是必须的，但是正确部署也非常重要。

这里再强调一下普遍存在的不安全的加密套件的问题，是体检中发现的重灾区，主要是没有关闭不安全的 TLS1.0 和 1.1 和一些弱强度加密套件。浏览器同服务器握手协商加密算法理论上是优先使用高强度的加密套件和加密算法，但是如果服务器不关闭不安全的加密算法和加密套件，等于告诉攻击者服务器接受采用不安全的加密算法实现加密通信，而弱加密强度的加密很容易被破解使得 SSL 证书加密失去了加密的意义，必须关闭所有不安全的加密套件！

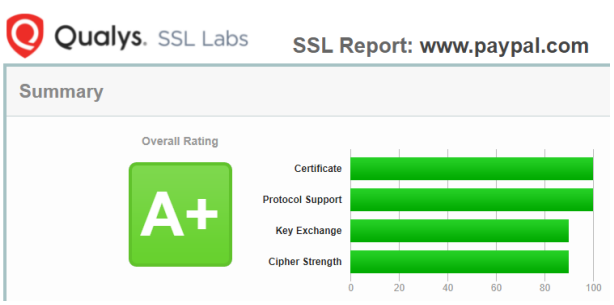
第三方支付 (排名不分先后)	评级	安全重新协议	关闭不安全协议	关闭不安全和弱强度加密套件	完整证书链	**DNS CAA 支持**
支付宝 ALIPAY	**B**	支持	没有关闭 TLS 1.0/1.1	没有关闭 10 个弱强度套件 **支持降级攻击防护**	是	不支持
财付通	**B**	支持	没有关闭 TLS 1.0/1.1	没有关闭 24 个弱强度套件 **支持降级攻击防护**	是，锚错误	不支持
银联商务 ChinaUMS	**A+**	支持	没有关闭 TLS 1.0/1.1 **支持 TLS 1.3**	没有关闭 23 个弱强度套件 **支持 HSTS，支持前向安全，支持降级攻击防护**	是，锚错误，	不支持
拉卡拉	**B**	支持	没有关闭 TLS 1.0/1.1	没有关闭 7 个弱强度套件，**支持降级攻击防护**	是，锚错误	不支持
通联支付 ALLINPAY	**B**	支持	没有关闭 TLS 1.0/1.1	没有关闭 23 个弱强度套件，**支持降级攻击防护**	是，锚错误	不支持
京东支付 JDPAY.COM	**B**	支持	没有关闭 TLS 1.0/1.1	没有关闭 10 个弱强度套件，**支持 HSTS，支持降级攻击防护**	是，锚错误	不支持
度小满	**B**	支持	没有关闭 SSL 3, TLS 1.0/1.1	没有关闭 4 个弱强度套件，没有关闭不安全协议 RC4，**支持降级攻击防护**	是	不支持

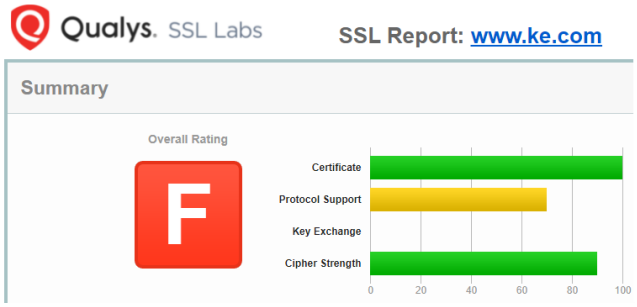
和包	B	支持	没有关闭 TLS 1.0/1.1 **支持 TLS 1.3**	没有关闭 24 个弱强度套件，**支持降级攻击防护**	是，锚错误	不支持
翼支付	B	支持	没有关闭 TLS 1.0/1.1 **支持 TLS 1.3**	没有关闭 23 个弱强度套件，**支持降级攻击防护，支持前向安全**	是，锚错误	不支持
沃支付	B	支持	没有关闭 TLS 1.0/1.1 **支持 TLS 1.3**	没有关闭 14 个弱强度套件，**支持 HSTS，支持降级攻击防护**	是	不支持

电商网站 (排名不分先后)	评级	安全重新协议	关闭不安全协议	关闭不安全和弱强度加密套件	完整证书链	**DNS CAA 支持**
天猫 TMALL.COM	B	支持	没有关闭 TLS 1.0/1.1	没有关闭 11 个弱强度套件 **支持 HSTS，支持降级攻击防护**	是	不支持
JD.京东 .COM	B	支持	没有关闭 TLS 1.0/1.1 **支持 TLS 1.3**	没有关闭 14 个弱强度套件 **支持 HSTS**(太短)	是	不支持
苏宁易购 suning.com	B	支持	没有关闭 TLS 1.0/1.1	没有关闭 16 个弱强度套件 **支持 HSTS**(太短)，**支持降级攻击防护**	是，锚错误，多余证书	不支持
美团 meituan.com	B	支持	没有关闭 TLS 1.0/1.1	没有关闭 14 个弱强度套件，**支持降级攻击防护**	是，锚错误	不支持
拼多多	B	支持	没有关闭 TLS 1.0/1.1	没有关闭 24 个弱强度套件，**支持降级攻击防护**	是	不支持
mi	B	支持	没有关闭 TLS 1.0/1.1 **支持 TLS 1.3**	没有关闭 10 个弱强度套件，**支持降级攻击防护**	是	不支持
滴滴	B	支持	没有关闭 TLS 1.1	没有关闭 22 个弱强度套件，**支持降级攻击防护**	是	不支持
携程	B	支持	没有关闭 TLS 1.0/1.1 **支持 TLS 1.3**	没有关闭 12 个弱强度套件，**支持降级攻击防护，支持 HSTS**(太短)	是	不支持
点点	B	支持	没有关闭 TLS 1.0/1.1 **支持 TLS 1.3**	没有关闭 14 个弱强度套件，**支持降级攻击防护**	是，锚错误	不支持
贝壳	F	支持	没有关闭 SSL 3, TLS 1.0/1.1	没有关闭匿名套件，弱密钥交换等，没有关闭 23 个弱强度套件和 3 个不安全套件，**支持降级攻击防护**	是	不支持

最后，给大家看看得分为 A+的第三方支付网站 PayPal 网站的体检结果截图(得分 A+)和得

分为 F 的贝壳网站的体检结果截图。笔者需要在这里特别声明的是：笔者不是故意要公开披露某个网站部署 SSL 证书存在的安全漏洞，这些漏洞说和不说都是摆在所有人(包括攻击者)的面前，任何人都可以使用各种安全扫描工具包括笔者使用的 Qualys SSL 体检系统来发现这些安全漏洞。





希望本文能再次引起各大第三方支付网站和电商网站的高度关注，及时把安全漏洞堵住。也希望熟悉这些网站的 IT 主管的朋友能把此文转发给相关网站主管。由于时间关系，我并没有遍历所有第三方支付网站和所有电商网站的 SSL 证书部署情况，其他网站也一定存在各种各样的 SSL 证书部署安全问题，大家都可以自己使用 SSL 体检工具发现这些问题并及时修复这些问题，希望通过大家的共同努力能提升我国互联网的整体安全水平。

王高华

2022 年 1 月 17 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。