Vulnérabilité du SSL 3.0 : faille Pood

Guide des mesures applicables aux marchands

Aperçu

Qu'est-ce que Poodle ?

Poodle est le nom d'une nouvelle faille de sécurité Internet affectant SSL 3.0 (Secure Sockets Layer), un protocole conçu pour sécuriser les connexions Internet. L'exploitation de cette vulnérabilité permet aux cybercriminels d'accéder à des connexions censées être sécurisées par l'intermédiaire de ce protocole de sécurité particulièrement exploité, mais vieux de 15 ans.

Quelles sont les mesures prises par PayPal ?

Nous allons intégralement cesser notre prise en charge du SSL 3.0 le **3 décembre 2014**. Nous sommes toutefois conscients qu'une telle décision peut engendrer des problèmes de compatibilité pour certains clients, les empêchant de payer avec PayPal sur les sites de marchands, entre autres conséquences. Pour évaluer votre situation et trouver une solution à vos difficultés éventuelles, nous avons créé ce *Guide des mesures applicables aux marchands*. Utilisez-le pour vérifier que votre intégration n'est pas menacée par cette vulnérabilité.

Nous vous tiendrons informé des mesures à venir sur les réseaux appropriés, y compris sur PayPal Forward, notre page Twitter et par l'intermédiaire de notre Service clientèle et de notre équipe Solutions e-commerce. Merci pour votre patience et votre compréhension. Nous faisons tout notre possible pour préserver la sécurité de vos informations financières.

Ce que vous devez faire...

Si vous ne gérez pas vous-même votre site ou votre intégration PayPal, nous vous conseillons de travailler en collaboration avec votre fournisseur de services (développeur, hôte, plateforme e-commerce, etc.) et de lui communiquer ce *Guide des mesures applicables aux marchands* dans lequel il trouvera toutes les informations nécessaires pour assurer la transition vers le TLS. Si votre fournisseur de services a des questions ou besoin d'aide, il peut contacter notre assistance technique marchands sur www.paypal.com/mts.

1. Testez votre intégration actuelle dans l'environnement de test PayPal

Si vous disposez d'une intégration directe avec PayPal, procédez comme suit :

NOTE: Nous travaillons directement avec nos partenaires pour résoudre la situation. Si vous avez procédé à l'intégration PayPal via un partenaire ou un système tiers, nous vous conseillons de travailler en collaboration avec les personnes appropriées pour vérifier que le protocole SSL 3.0 n'est plus utilisé. Si vous utilisez des composants téléchargeables ou une solution non hébergée, vous devrez peut-être en télécharger la dernière version disponible.

a. Dirigez-vous vers notre environnement de test : https://developer.paypal.com/docs/classic/lifecycle/ug_sandbox/

   - Le SSL 3.0 ayant déjà été désactivé dans l'environnement de test PayPal, si vous arrivez à lancer une requête API (interface de programmation), c'est que vous ne l'utilisez pas.

b. Si votre requête n'aboutit pas, vérifiez vos journaux pour en connaître la raison.

   - Si vous repérez une erreur similaire à celles indiquées ci-dessous, c'est que vous utilisez le SSL 3.0. Vous devrez alors configurer votre connexion sécurisée pour le remplacer par le TLS (Transport Layer Security).

```
* Erreur protocole SSL inconnu, échec de la connexion sécurisée à api-
3t.sandbox.paypal.com:-9824
```

OU

```
140062736746144:error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version
number:s3_pkt.c:337:
...
Nouveau, (AUCUN), Chiffrage (AUCUN)
Renégociation sécurisée non prise en charge
Compression : AUCUNE
Expansion : AUCUNE
Session SSL :
Protocole : SSLv3
...
```

2. Passez au TLS

Tous les utilisateurs PayPal doivent désactiver le SSL 3.0 pour leurs interactions clients et passer au TLS avant le 3 décembre 2014. Le tableau suivant contient des instructions de base permettant de remplacer le SSL par le TLS grâce à l'utilisation de langages et modes de connexion courants. Les paramètres exacts peuvent varier en fonction de votre installation...

NOTE: Pour en savoir plus sur la mise à niveau des kits de développement PayPal et les langages listés ci-dessous, rendez-vous sur https://ppmts.custhelp.com/app/answers/detail/a_id/1182.

<table>
<tr><th>Mode de connexion</th><th>Action</th></tr>
<tr><td>Kit de développement PayPal</td><td>Aucune version ni aucun langage actuel du kit de développement PayPal n'utilisent le SSL 3.0. Toutefois, les kits de développement PHP et Java ayant récemment été mis à jour pour faire face à la situation, tous les marchands doivent télécharger les dernières versions disponibles (ultérieures au 21 octobre 2014). Si vous ne savez pas quelle version du kit de développement vous utilisez, testez votre intégration dans notre environnement de test comme expliqué dans l'étape 1.
Pour en savoir plus sur les différentes versions du kit de développement, rendez-vous sur http://paypal.github.io/sdk/#merchant</td></tr>
<tr><td>Point de terminaison API</td><td>Vérifiez que vous vous connectez aux points de terminaison API de PayPal via le TLS 1.0 ou 1.2 (tous les points de terminaison ne sont pas pris en charge par le TLS 1.1 pour le moment). Consultez les éléments ci-dessous pour configurer le protocole TLS pour le langage que vous utilisez. Si votre environnement le prend en charge, ne codez pas de version TLS spécifique, car le protocole décidera de la version la plus récente automatiquement.
<table>
<tr><th>Langage</th><th>Action</th></tr>
<tr><td>Ruby</td><td>Définissez le protocole TLS sur OpenSSL::SSL::SSLContext.
Pour en savoir plus, rendez-vous sur http://ruby-doc.org/stdlib-1.9.3/libdoc/openssl/rdoc/OpenSSL/SSL/SSLContext.html</td></tr>
<tr><td>Python</td><td>Configurez le protocole TLS sur ssl.SSLContext.
Pour en savoir plus, rendez-vous sur https://docs.python.org/2/library/ssl.html#ssl.SSLContext</td></tr>
<tr><td>Node.js</td><td>Utilisez la limite de renégociation correcte comme indiqué ici :
http://nodejs.org/api/tls.html#tls_client_initiated_renegotiation_attack_mitigation</td></tr>
<tr><td>PHP</td><td>Modifiez CURLOPT_SSLVERSION en CURL_SSLVERSION_TLSv1 dans vos options cURL.
Pour en savoir plus, rendez-vous sur http://curl.haxx.se/libcurl/c/CURLOPT_SSLVERSION.html</td></tr>
<tr><td>Java</td><td>Configurez le protocole TLS sur javax.net.ssl.SSLContext.</td></tr>
</table>
</td></tr>
</table>

		• Pour en savoir plus, rendez-vous sur http://docs.oracle.com/javase/7/docs/technotes/guides/security/jsse/JSSERefGuide.html
	C#	Utilisez SecurityProtocolType Tls. • Pour en savoir plus, rendez-vous sur http://msdn.microsoft.com/en-us/library/system.net.securityprotocoltype%28v=vs.110%29.aspx

3. Créez de nouveaux identifiants (facultatif)

Après être passé au TLS et l'avoir testé, vous pouvez créer de nouveaux identifiants API pour toutes vos requêtes API PayPal. Cette étape est fortement conseillée, mais pas obligatoire. Basez votre décision sur les risques encourus par votre entreprise et vos clients.

- Si vous utilisez un **certificat** d'authentification, vous n'avez rien à faire, car la vulnérabilité du protocole SSL 3.0 n'affecte par les certificats SSL.
- Si vous utilisez une authentification par **signature**, rendez-vous sur https://developer.paypal.com/docs/classic/api/apiCredentials/
- Si vous utilisez le protocole d'authentification **OAuth**, rendez-vous sur https://developer.paypal.com/docs/integration/admin/manage-apps/

Merci

Nous vous remercions de l'attention que vous portez à ce problème et de votre compréhension face à notre approche. Nous savons que notre décision peut créer des problèmes de compatibilité, mais nous tenons vraiment à souligner combien cette gêne temporaire nous permettra d'assumer nos engagements de sécurité envers nos utilisateurs.