Vulnerabilidad POODLE en el protocolo SSL 3.0

Guía de respuesta para vendedores

Descripción general

¿Qué es POODLE?

POODLE es una vulnerabilidad de seguridad de Internet que afecta al protocolo Secure Sockets Layer (SSL) 3.0, que se diseñó para garantizar la seguridad de las conexiones al navegar por Internet. Cuando se explota, esta vulnerabilidad permite a un ciberdelincuente obtener acceso a conexiones consideradas seguras a través de este protocolo de seguridad ampliamente utilizado (pero que tiene 15 años de antigüedad).

¿Cuál va a ser la respuesta de PayPal?

PayPal desactivará completamente la compatibilidad con SSL 3.0 **el 3 de diciembre de 2014**. Lamentablemente, somos conscientes de que la desconexión de SSL 3.0 puede ocasionar problemas de compatibilidad para algunos de nuestros clientes, lo que impedirá poder pagar con PayPal en los sitios web de algunos vendedores u otros problemas de procesamiento que aún estamos identificando. Para facilitarle la evaluación y posibles soluciones, hemos elaborado esta *Guía de respuesta para vendedores* con el fin de ayudarle a garantizar la seguridad de su integración frente a esta vulnerabilidad.

Tenemos previsto mantener informados a nuestros clientes acerca de como estamos tratando este problema a través de los canales adecuados, incluidos PayPal Forward, nuestra cuenta de Twitter y el Servicio de Atención al Cliente, y a los vendedores a través de nuestro equipo de Servicios para vendedores. Agradecemos su paciencia y comprensión, ya que trabajamos permanentemente para prestarle un mejor servicio y mantener su seguridad y la de nuestros consumidores.

Qué debe hacer…

Si no administra su sitio web ni la integración de PayPal, le recomendamos encarecidamente que trabaje con su partner de servicio del sitio web (programador, empresa de alojamiento, plataforma de comercio electrónico, etc.) y comparta esta *Guía de respuesta para vendedores*, que proporciona las pautas básicas para actualizar a TLS. Si su partner de servicio del sitio web tiene alguna duda o necesita asistencia, puede ponerse en contacto con nuestro equipo de asistencia técnica para vendedores en www.paypal.com/mts.

1. Pruebe su integración actual en el Entorno de pruebas de PayPal.

Si la integración se encuentra directamente en PayPal, siga los pasos siguientes:

NOTE: Estamos trabajando con nuestros partners para resolver el problema del protocolo SSL 3.0. Si su integración se ha realizado a través de un partner o del sistema de un tercero, le recomendamos que trabaje con su partner para asegurarse de que dejen de utilizar SSL 3.0. Si utiliza componentes descargables o una solución no alojada, tal vez deba actualizarlos o descargar la versión más reciente.

a. Dirija su entorno de prueba al nuestro: https://developer.paypal.com/docs/classic/lifecycle/ug_sandbox/.

   - SSL 3.0 ya se ha desactivado en el Entorno de pruebas de PayPal, por lo que si puede realizar correctamente una solicitud de interfaz de programación de aplicaciones (API) no está utilizando SSL 3.0.

b. Si la solicitud falla, compruebe los registros para ver el motivo.

- Si detecta un error similar a los que se muestran a continuación, está utilizando SSL 3.0 y tendrá que configurar su conexión segura para utilizar Seguridad de la capa de transporte (TLS).

```
* Unknown SSL protocol error in connection to api-3t.sandbox.paypal.com:-9824
```

O

```
140062736746144:error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version
number:s3_pkt.c:337:
...
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol: SSLv3
...
```

2. Actualización a TLS

Todos los clientes de PayPal deben haber desactivado SSL 3.0 para las interacciones con clientes y haber actualizado a TLS el 3 de diciembre de 2014. En la tabla siguiente se ofrecen las directrices básicas sobre cómo actualizar a TLS con métodos de conexión y lenguajes comunes. Su configuración exacta podría variar.

NOTE: Para obtener instrucciones detalladas de actualización de los SDK y de los lenguajes que se indican a continuación en https://ppmts.custhelp.com/app/answers/detail/a_id/1182.

<table>
<tr><th>Método de conexión</th><th>Acción</th></tr>
<tr><td>PayPal SDK</td><td>Ningún lenguaje ni versión actual del kit de programación de software (SDK) de PayPal utiliza SSL. Sin embargo, dado que los SDK de Java y PHP se han actualizado recientemente para solucionar este problema, todos los vendedores que utilizan estos SDK o SDK heredados (anteriores al 21 de octubre de 2014) tendrán que actualizar a la última versión. Si no está seguro de si está utilizando el último SDK, pruebe su integración en el entorno de pruebas, tal como se explica en el paso 1.
Para obtener información sobre las últimas versiones del SDK, consulte: http://paypal.github.io/sdk/</td></tr>
<tr><td>Punto final de API</td><td>Asegúrese de se conecta a los puntos finales de PayPal con TLS. Vea la tabla siguiente para configurar el protocolo TLS para el lenguaje que utilice. Si su entorno lo admite, no codifique ninguna versión concreta de TLS, ya que el protocolo decidirá automáticamente cuál es la versión más reciente posible.
<table>
<tr><th>Lenguaje</th><th>Acción</th></tr>
<tr><td>Ruby</td><td>Configure el protocolo TLS en OpenSSL::SSL::SSLContext.
Para obtener más información, consulte: http://ruby-doc.org/stdlib-1.9.3/libdoc/openssl/rdoc/OpenSSL/SSL/SSLContext.html</td></tr>
<tr><td>Python</td><td>Configure el protocolo TLS en ssl.SSLContext.
Para obtener más información, consulte: https://docs.python.org/2/library/ssl.html#ssl.SSLContext</td></tr>
<tr><td>Node.js</td><td>Utilice el límite de renegociación correcto según lo especificado aquí:
http://nodejs.org/api/tls.html#tls_client_initiated_renegotiation_attack_mitigation</td></tr>
<tr><td>PHP</td><td>Configure CURLOPT_SSLVERSION a CURL_SSLVERSION_TLSv1 en sus opciones de Curl.
Para obtener más información, consulte: http://curl.haxx.se/libcurl/c/CURLOPT_SSLVERSION.html</td></tr>
</table>
</td></tr>
</table>

	Java	Configure el protocolo TLS en javax.net.ssl.SSLContext. • Para obtener más información, consulte: http://docs.oracle.com/javase/7/docs/technotes/guides/security/jsse/JSSERefGuide.html
	C#	Utilice TLS SecurityProtocolType. • Para obtener más información, consulte: http://msdn.microsoft.com/en-us/library/system.net.securityprotocoltype%28v=vs.110%29.aspx

3. Emitir credenciales nuevas (opcional)

Una vez que haya probado y cambiado correctamente a TLS, es posible que desee volver a emitir y descargar nuevas credenciales de API para cualquier solicitud de la API de PayPal. Este paso es my aconsejable, aunque no obligatorio. Tome una decisión para su empresa y clientes en función de los riesgos.

- Si utiliza la autenticación **Certificate**, no es necesario realizar ninguna acción porque la vulnerabilidad está en el protocolo SSL 3.0 y no en el diseño de los certificados SSL.
- Si utiliza autenticación **Signature**, consulte: https://developer.paypal.com/docs/classic/api/apiCredentials/
- Si utiliza autenticación **OAuth**, consulte: https://developer.paypal.com/docs/integration/admin/manage-apps/

Gracias

Le agradecemos su pronta respuesta respecto a este problema y que entienda nuestro enfoque. Aunque reconocemos que este paso necesario puede provocar problemas de compatibilidad, no podemos dejar de destacar que este inconveniente a corto plazo se compensará notablemente por nuestra promesa conjunta a nuestros respectivos clientes de que mantendremos la seguridad de sus cuentas y datos financieros.