Seguridad para comercios

Guía de actualización del Sistema

Haga clic AQUÍ para obtener información
sobre el cumplimiento con el cifrado SHA-256.

Ayuda para preparar su integración para el futuro.

Las amenazas de seguridad mundiales evolucionan constantemente y la seguridad de nuestros comercios sigue siendo nuestra máxima prioridad. Para protegerse contra las amenazas tanto actuales como futuras, animamos a nuestros comercios a que realicen los cambios siguientes en sus integraciones:

1. Dejar de utilizar el certificado raíz G2 de VeriSign
2. Actualizar la integración para que sea compatible con los certificados que usan el algoritmo SHA-256

¿Por qué cambiar?

El sector de las autoridades públicas de certificación (CA) continúa mejorando la seguridad de los certificados SSL. Con vistas al momento en que se pida usar el algoritmo de firma SHA-256 en 2016, ya no se admitirá el certificado raíz VeriSign G2, usado tradicionalmente para conectarse a los puntos finales de la API de PayPal y Notificación de pago instantánea (IPN).

¿Cuándo debo actuar?

Le recomendamos que actúe tan pronto como sea posible para que pueda prepararse para estos cambios. Para conocer los plazos en detalle, incluidas las fechas de actualización para los puntos de acceso de la API activos y del entorno de pruebas Sandbox, consulte el Micrositio de cambio de Certificado SSL 2015-2016.

NOTE: Es importante tener en cuenta que estos cambios tienen como finalidad solucionar los problemas de seguridad del sector, y no son exclusivos de PayPal. Una vez implementados, mejorarán la privacidad y la confiabilidad de sus integraciones de PayPal. Debido a que los detalles de estos cambios varían en función del sistema, le recomendamos que se realicen con la ayuda de un administrador de sistemas cualificado.

1. Dejar de utilizar el certificado raíz G2 de VeriSign

El problema: En el pasado, VeriSign emitía certificados SSL que tenían una jerarquía de dos niveles firmada por un certificado raíz G2 de 1024 bits. En los últimos años, el gobierno y el sector de las CA públicas han cambiado a certificados de 2048 bits más seguros, por lo que ahora VeriSign emite certificados SSL que tienen una cadena de confianza firmada por un certificado raíz G5 de 2048 bits emitido en 2006.

Nuestra respuesta: De acuerdo con los estándares del sector, PayPal dejará de aceptar conexiones seguras a los puntos de acceso API/IPN que esperan que nuestro certificado/jerarquía de dos niveles estén firmados por el certificado raíz G2. Solo se realizarán correctamente las solicitudes de conexión segura que esperan que nuestro certificado o cadena de confianza esté firmado por el certificado raíz G5.

¿Qué debe hacer?

Deje de utilizar conexiones SSL que dependan de los certificados raíz de VeriSign con un identificador G2, si su sistema actualmente exige el uso de este certificado raíz específico. El sector trabaja activamente para retirar progresivamente los certificados raíz de 1024 bits este año.

- No se admiten las conexiones seguras que se basan en nuestra cadena de certificados firmada por el certificado raíz G2:

Unidad organizacional	Autoridad pública de certificación principal de clase 3: **G2**
Número de serie	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Huella digital del certificado SHA1	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Se admiten las conexiones seguras que se basan en nuestra cadena de certificados firmada por el certificado raíz G5:

Nombre común	Autoridad pública de certificación principal VeriSign Clase 3: **G5**
Número de serie	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Huella digital del certificado SHA1	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Siga estas pautas para garantizar que está conectándose de manera segura usando el Certificado raíz VeriSign G5:

1. **Compruebe el almacén de certificados.** Pídale al host de su sitio web o administrador del sistema que comprueben si el Certificado raíz VeriSign G5 está incluido en el almacén raíz que utiliza su código para la lógica de validación. Si es así, no se necesita ninguna acción.
    - Consulte los siguientes vínculos para comprobar si dispone en su almacén de claves del certificado raíz G5 con Java, Linux o Windows.
2. **Compruebe sus registros de errores.** Si no se ha descargado el Certificado raíz VeriSign G5 para reemplazar al Certificado raíz G2, podría ver mensajes de error similares al siguiente:
    - Error de protocolo de enlace SSL: “No trusted certificate found” (No se ha encontrado ningún certificado de confianza)
    - Código de resultado -31: “The certificate chain did not validate, no local certificate found” (La cadena de certificados no se validó; no se ha encontrado ningún certificado local)
    - Código de resultado -8: “SSL connection failed” (Error de conexión SSL)
    - Error -1

    Para resolver estos problemas, realice uno de los siguientes pasos:
    - Actualice su software a la versión más reciente compatible con SHA-256.
    - Si se utiliza un almacén de claves para la validación/autenticación de certificados, instale el certificado raíz VeriSign G5 en su almacén de claves.
3. **Obtenga un certificado raíz VeriSign G5.** Si su almacén de certificados o cliente de Java no incluye el Certificado raíz VeriSign G5, entonces pídale a su administrador del sistema descargarlo de VeriSign y guardarlo en el almacén de certificados, así como cualquier otro paquete de autenticación con conexión SSL.
    - Descargar el certificado raíz VeriSign G5 de Symantec
    - Descargar certificados SSL específicos del servidor (si su servidor lo requiere)

2. Actualizar al algoritmo de firma SHA-256

El problema: SHA-1 es un algoritmo criptográfico de 22 años de antigüedad que se está viendo amenazado por el aumento de la potencia informática. SHA-256 utiliza un algoritmo más sólido con valores hash de 256 bits.

Nuestra respuesta: PayPal actualizará los certificados SSL en todos los extremos activos y

¿Qué debe hacer?

Siga estas pautas para la transición de utilizar certificados SSL que utilizan el algoritmo de firma SHA-1 al algoritmo de firma más consistente SHA-256:

1. **Compruebe el entorno.** Asegúrese de que su entorno admite los certificados SHA-256.
   - Para obtener una lista de hardware y software admitidos, consulte recursos en Internet, como la Guía de compatibilidad SHA-2 de DigiCert y la Lista de servidores y navegadores compatibles de Symantec.
   - Si hay partes de su entorno que no admiten SHA-256, debe sustituirlas o cambiarlas antes de poder instalar los certificados nuevos.
   - Windows 2000 Server y algunas versiones de Windows XP pueden ser incompatibles con SHA-2. Este blog de PKI de Windows sobre SHA2 y Windows puede ayudarle a actualizar su entorno con parches y recomendaciones.
2. **Compruebe los certificados.** Si su entorno admite SHA-256, asegúrese de tener el certificado raíz VeriSign G5 en su almacén de claves.

¿Dudas?

Para conocer más detalles y ver las preguntas frecuentes, consulte el micrositio de Cambio de certificado SSL 2015-2016.

¡Gracias!

Agradecemos que preste atención inmediata a este problema y que entienda nuestra postura. Aunque reconocemos que estos pasos necesarios pueden provocar problemas de compatibilidad, no podemos dejar de destacar que este inconveniente a corto plazo se compensa en gran medida con nuestra promesa a nuestros respectivos clientes de que mantendremos la seguridad de sus cuentas y su información financiera.