Sicherheit für Händler

Leitfaden zum Systemupgrade

Klicken Sie HIER für Informationen über die SHA-256-Compliance.

Integration für die Zukunft rüsten

Da sich die globale Bedrohungslage fortlaufend verändert, bleibt die Sicherheit unserer Händler eine unserer wichtigsten Prioritäten. Wir empfehlen allen Händlern, ihre Integrationen wie folgt zu aktualisieren, um sich gegen derzeitige und künftige Bedrohungen zu schützen:

1. Verwendung des VeriSign G2-Root-Zertifikats einstellen
2. Integration für die Unterstützung von Zertifikaten mit Algorithmus SHA-256 aktualisieren

Weshalb diese Änderungen?

Die öffentlichen Zertifizierungsstellen (CA) arbeiten fortlaufend an der Verbesserung der Sicherheit von SSL-Zertifikaten. Im Rahmen der Vorbereitung auf die Einführung des neuen Verschlüsselungsalgorithmus SHA-256 im Jahr 2016 wird die Unterstützung des ursprünglich für Verbindungen zu PayPal-API- und IPN-Endpunkten für die sofortige Zahlungsbestätigung verwendete VeriSign G2-Root-Zertifikat eingestellt.

Wann muss ich handeln?

Wir empfehlen, so schnell wie möglich zu handeln, um sich auf diese Veränderungen vorzubereiten. Einen ausführlicher Zeitplan mit den Upgrade-Terminen für Live- und Sandbox-API-Endpunkte finden Sie auf der Microsite zu Änderungen an SSL-Zertifikaten 2015-2016.

NOTE: Beachten Sie, dass diese Änderungen auf branchenweite Sicherheitsmaßnahmen zurückgehen und nicht speziell von PayPal initiiert wurden. Durch die Implementierung werden der Datenschutz und die Zuverlässigkeit Ihrer PayPal-Integration deutlich verbessert. Da die Details dieser Änderungen je nach System variieren, empfehlen wir, diese mit Unterstützung eines qualifizierten Systemadministrators vorzunehmen.

1. Verwendung des VeriSign G2-Root-Zertifikats einstellen

Das Problem: In der Vergangenheit stellte VeriSign SSL-Zertifikate mit einer Vertrauenskette aus, die durch ein G2-Root-Zertifikat mit 1024 Bit verschlüsselt wurde. In den letzten Jahren haben öffentliche Zertifizierungsstellen auf sicherere Zertifikate mit 2048 Bit umgestellt, weshalb VeriSign nun SSL-Zertifikate mit einer Vertrauenskette ausstellt, die durch ein 2006 ausgestelltes G5-Root-Zertifikat mit 2048 Bit verschlüsselt wird.

Unsere Reaktion: Gemäß den Vorgaben der Branche akzeptiert PayPal künftig keine sicheren Verbindungen zu den API/IPN-Endpunkten mehr, für die unser Zertifikat/unsere Vertrauenskette durch das G2-Root-Zertifikat verschlüsselt werden muss. Nur sichere Verbindungsanforderungen, für die unser Zertifikat/unsere Vertrauenskette durch das G5-Root-Zertifikat verschlüsselt werden muss, führen dann zum erfolgreichen Aufbau sicherer Verbindungen.

Was müssen Sie tun?

Stellen Sie die Nutzung von SSL-Verbindungen mit VeriSign G2-Root-Zertifikat ein, sofern Ihr System aktuell die Verwendung dieses Root-Zertifikats erfordert. Die Branchenakteure arbeiten aktiv an der Einstellung der Unterstützung von Root-Zertifikaten mit 1024 Bit in diesem Jahr.

- Sichere Verbindungen, für die unsere Zertifikatskette durch das G2-Root-Zertifikat verschlüsselt werden muss, werden nicht unterstützt:

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

- Sichere Verbindungen, für die unsere Zertifikatskette durch das G5-Root-Zertifikat verschlüsselt werden muss, werden unterstützt:

Allgemeine Bezeichnung	VeriSign Class 3 Public Primary Certification Authority - **G5**
Seriennummer	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
SHA1-Fingerprint des Zertifikats	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Beachten Sie die folgenden Schritte für den Aufbau sicherer Verbindungen mit einem unterstützten VeriSign G5-Root-Zertifikat:

1. **Überprüfen Sie Ihren Zertifikatsspeicher.** Lassen Sie Ihren Webhost oder Systemadministrator überprüfen, ob sich das VeriSign G5-Root-Zertifikat in dem Root-Speicher befindet, der von Ihrem Code für die Validierungslogik verwendet wird. Ist dies der Fall, sind keine weiteren Maßnahmen erforderlich.
    - Überprüfen Sie über die folgenden Links, ob sich das G5-Root-Zertifikat in Ihrem Schlüsselspeicher befindet. Wählen Sie dazu je nach System Java, Linux oder Windows.
2. **Überprüfen Sie Ihre Fehlerprotokolle.** Wenn das VeriSign G5-Root-Zertifikat nicht heruntergeladen wurde, um das G2-Root-Zertifikat zu ersetzen, erhalten Sie möglicherweise folgende Fehlermeldungen:
    - SSL-Handshake-Fehler "No trusted certificate found"
    - Ergebniscode -31 "The certificate chain did not validate, no local certificate found”
    - Ergebniscode -8 "SSL connection failed"
    - -1 Fehler

    Führen Sie einen der folgenden Schritte aus, um diese Probleme zu lösen:

    - Aktualisieren Sie Ihre Software auf die neueste Version, die SHA-256 unterstützt.
    - Wird ein Schlüsselspeicher für die Validierung/Authentifizierung des Zertifikats verwendet, installieren Sie das VeriSign G5-Root-Zertifikat in Ihrem Schlüsselspeicher.
3. **Laden Sie ein VeriSign G5-Root-Zertifikat herunter.** Wenn Ihr Zertifikatsspeicher oder Java-Client das VeriSign G5-Root-Zertifikat noch nicht enthält, lassen Sie Ihren Systemadministrator dieses Zertifikat bei VeriSign herunterladen und im Zertifikatsspeicher ablegen. Dasselbe gilt für alle anderen Authentifizierungspakete für SSL-Verbindungen.
    - VeriSign G5-Root-Zertifikat von Symantec herunterladenVeriSign G5-Root-Zertifikat von Symantec herunterladen

- Serverspezifische SSL-Zertifikate Serverspezifische SSL-Zertifikate herunterladen, falls für Ihren Server erforderlich

2. Auf Verschlüsselungsalgorithmus SHA-256 aktualisieren

Das Problem: SHA-1 ist ein 22 Jahre alter Kryptoalgorithmus, dem die zunehmende Rechenleistung immer mehr zusetzt. SHA-256 verwendet dagegen einen stärkeren Algorithmus mit 256-Bit-Hashwerten.

Unsere Reaktion: PayPal aktualisiert Mitte 2016 die SSL-Zertifikate aller Live- und Sandbox-Endpunkte von SHA-1 auf den stärkeren und robusteren Algorithmus SHA-256.

Was müssen Sie tun?

Führen Sie die folgenden Schritte aus, um den Verschlüsselungsalgorithmus Ihrer SSL-Zertifikate von SHA-1 auf SHA-256 zu aktualisieren:

1. **Überprüfen Sie Ihre Umgebung.** Stellen Sie sicher, dass Ihre Umgebung SHA-256-Zertifikate unterstützt.
   - Eine Liste der unterstützten Hardware und Software finden Sie in Online-Ressourcen, wie dem SHA-2 Compatibility Guide von DigiCert und der Supported Browser and Server List von Symantec.
   - Wenn Teile Ihrer Umgebung SHA-256 nicht unterstützen, müssen Sie diese austauschen oder aktualisieren, bevor Sie die neuen Zertifikate implementieren können.
   - Windows 2000 Server und einige Versionen von Windows XP sind möglicherweise nicht mit SHA-2 kompatibel. In diesem Windows PKI-Blog zu SHA2 unter Windows finden Sie Patches und Empfehlungen zur Aktualisierung Ihrer Umgebung.
2. **Überprüfen Sie Ihre Zertifikate.** Wenn Ihre Umgebung SHA-256 unterstützt, stellen Sie sicher, dass sich das VeriSign G5-Root-Zertifikat in Ihrem Schlüsselspeicher befindet.

Sie haben weitere Fragen?

Weitere Details und häufig gestellte Fragen finden Sie auf der Microsite zu Änderungen an SSL-Zertifikaten 2015-2016.

Vielen Dank!

Danke, dass Sie sich diesem Problem umgehend widmen und uns bei der Lösung unterstützen. Uns ist bewusst, dass diese wichtigen Maßnahmen zu Kompatibilitätsproblemen führen können. Dennoch können wir nicht genug betonen, dass die kurzfristige Unannehmlichkeit durch eine nachhaltige Wahrung der Sicherheit aller Kundendaten mehr als aufgewogen wird.