Mağaza Güvenliği

Sistem Yükseltme Kılavuzu

SHA-256 uyumluluğuna ilişkin bilgi için BURAYI tıklayın.

Entegrasyonunuzu Zamana Karşı Koruyun

Küresel güvenlik tehditleri sürekli olarak değişiyor ve mağazalarımızın güvenliği en önemli önceliğimiz olmaya devam ediyor. Şu andaki ve gelecekteki tehditlere karşı koruma sağlamak için mağazalarımızı, entegrasyonlarına aşağıdaki yükseltmeleri uygulamaları konusunda teşvik ediyoruz:

1. VeriSign G2 Kök Sertifikasını kullanmayı bırakın
2. SHA-256 algoritmasını kullanan sertifikaları desteklemesi için entegrasyonunuzu güncelleyin

Neden değiştirilmeli?

Ortak Sertifika Yetkilisi (CA) sektörü, SSL sertifikalarının güvenliğini iyileştirmeye devam ediyor. 2016 yılında SHA-256 imza algoritmasının kullanım gerekliliğine hazır olmak adına, tarih boyunca PayPal API ve Anında Ödeme Bildirimi (IPN) uç noktalarına bağlanmak için kullanılan VeriSign G2 Kök sertifikası artık desteklenmeyecektir.

Ne zaman yapmam gerekiyor?

Bu değişikliklere yönelik hazırlık yapmak için en hızlı şekilde harekete geçmenizi öneririz. Canlı ve Sandbox Test Ortamı API uç noktalarının güncelleme tarihleri dahil ayrıntılı zaman çizelgesi için bkz. 2015-2016 SSL Sertifika Değişikliği Mikro Sitesi.

NOTE: Bu değişikliklerin sektör genelindeki güvenlik sorunlarını çözmek için olduğuna ve PayPal'a özgü olmadığına dikkat edilmesi önemlidir. Değişiklikler uygulandıklarında, PayPal entegrasyonlarınızın gizliliğini ve güvenilirliğini iyileştireceklerdir. Bu değişikliklerin ayrıntıları sistemlere göre farklılık gösterdiğinden, yetkili bir sistem yöneticisinin yardımı ile yapılmasını öneririz.

1. VeriSign G2 Kök Sertifikasını kullanmayı bırakın

Sorun: VeriSign geçmişte, 1024-bit G2 Kök Sertifikası ile imzalı bir güven zinciri olan SSL sertifikalarını oluşturdu. Son yıllarda, hükümet ve Ortak CA sektörü daha güvenli olan 2048-bit sertifikalarına geçti, bu nedenle VeriSign artık 2006 yılında oluşturulan 2048-bit G5 Kök Sertifikası imzalı bir güven zinciri olan SSL sertifikalarını oluşturuyor.

Yanıtımız: Sektör standartları uyarınca, PayPal bundan sonra sertifikamızın/güven zincirimizin G2 Kök Sertifikası imzalı olmasını bekleyen API/IPN uç noktalarına güvenli bağlantıları kabul etmeyecektir. Yalnızca sertifikamızın/güven zincirimizin G5 Kök Sertifikası imzalı olmasını bekleyen güvenli bağlantı taleplerinin sonucunda başarılı güvenli bağlantılar elde edilebilecektir.

Yapmanız gerekenler...

Sisteminiz şu anda özellikle bu Kök Sertifikasının kullanılmasını zorunlu kılıyorsa, G2 tanımlayıcılı VeriSign Kök Sertifikalarına dayanan SSL bağlantılarını kullanmayı bırakın. 1024-bit Kök Sertifikalarını bu yıl aşamalı olarak sona erdirmek için sektörde aktif bir çalışma sürdürülüyor.

- Sertifika zincirimizin G2 Kök Sertifikası imzalı olmasına dayanan güvenli bağlantılar desteklenmemektedir:

Kuruluş Birimi	Sınıf 3 Ortak Ana Sertifika Yetkilisi - **G2**
Seri Numarası	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Sertifika SHA1 Parmak İzi	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Sertifika zincirimizin G5 Kök Sertifikası imzalı olmasına dayanan güvenli bağlantılar desteklenmektedir:

Ortak Ad	VeriSign Sınıf 3 Ortak Ana Sertifika Yetkilisi - **G5**
Seri Numarası	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Sertifika SHA1 Parmak İzi	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Desteklenen bir VeriSign G5 Kök Sertifikası ile güvenli bir şekilde bağlandığınızdan emin olmak için şu talimatlara uyun:

1. **Sertifika deponuzu kontrol edin.** Web sitesi barındırıcınızın veya sistem yöneticinizin VeriSign G5 Kök Sertifikasının doğrulama mantığı kodunuz tarafından kullanılan kök deposuna dahil olduğunu teyit etmesini isteyin. Öyle ise, hiçbir işlem yapılmasına gerek yoktur.
    - G5 Kök Sertifikasının olup olmadığını öğrenmek üzere anahtar mağazanızı kontrol etmek için bkz. Java için, Linux için veya Windows için.
2. **Hata dökümlerinizi kontrol edin.** VeriSign G5 Kök Sertifikası, G2 Kök Sertifikasının yerine indirilmediyse, aşağıdakine benzer hata mesajları görebilirsiniz:
    - SSL el sıkışma hatası, “Güvenli sertifika bulunamadı”
    - Sonuç kodu -31, “Sertifika zinciri doğrulanmadı, yerel sertifika bulunamadı”
    - Sonuç kodu -8, “SSL bağlantısı başarısız”
    - -1 hatası

    Bu sorunları çözmek için şunlardan birini yapın:

    - Yazılımınızı SHA-256'yı destekleyen en son sürüme güncelleyin.
    - Sertifika doğrulaması için bir anahtar mağazası kullanılıyorsa, VeriSign G5 Kök Sertifikasını anahtar mağazanıza yükleyin.
3. **Bir VeriSign G5 Kök Sertifikası alın.** Sertifika deponuz veya Java müşteriniz VeriSign G5 Kök Sertifikasını içermiyorsa, sistem yöneticinizden bunu VeriSign'dan indirmesini ve diğer tüm SSL bağlantı doğrulama paketleriyle birlikte sertifika deponuza kaydetmesini isteyin.
    - Symantec'in VeriSign G5 Kök Sertifikasını indirinSymantec'in VeriSign G5 Kök Sertifikasını indirin
    - Sunucunuz gerekli kılıyorsa, belirli sunucu sertifikalarını indirin

2. SHA-256 imza algoritmasına güncelleyin

Sorun: SHA-1, bilgi işlem gücündeki artışlar nedeniyle tehdit altında olan 22 yıllık bir kriptografik algoritmadır. SHA-256, 256-bit karma değerleri ile daha güçlü bir algoritma kullanmaktadır.

Yanıtımız: PayPal, 2016 yılının ortalarında tüm Canlı ve Test Ortamı uç noktalarındaki SSL sertifikalarını SHA-1'den daha güçlü ve sağlam olan SHA-256'ya yükseltiyor.

Yapmanız gerekenler…

SHA-1 imza algoritmasını kullanan SSL sertifikalarından, daha güçlü olan SHA-256 imza algoritmasına geçiş yapmak için aşağıdaki talimatlara uyun:

1. **Ortamınızı kontrol edin.** Ortamınızın SHA-256 sertifikaları desteklediğinden emin olun.
   - Desteklenen donanım ve yazılım listesi için online kaynaklara başvurun, örneğin: DigiCert'in SHA-2 Uyumluluk Kılavuzu ve Symantec'in Desteklenen Tarayıcı ve Sunucu Listesi.
   - Ortamınızın parçaları SHA-256'yı desteklemiyorsa, yeni sertifikaları uygulamadan önce bu parçaları değiştirmeli veya yükseltmelisiniz.
   - Windows 2000 Server ve Windows XP'nin bazı sürümleri SHA-2 ile uyumlu olmayabilir. SHA2 ve Windows konusundaki Windows PKI bloğu ortamınızı yükseltme önerileri ve yamalarla birlikte size yardımcı olabilir.
2. **Sertifikalarınızı kontrol edin..** Ortamınız SHA-256'yı destekliyorsa, anahtar mağazanızda VeriSign G5 Kök Sertifikası olduğundan emin olun.

Daha fazla sorunuz mu var?

Daha fazla ayrıntı ve sık sorulan sorular için lütfen bkz.
2015-2016 SSL Sertifika Değişikliği Mikro Sitesi.

Teşekkür Ederiz!

Bu soruna hemen dikkat gösterdiğiniz ve yaklaşımımızı anlayışla karşıladığınız için teşekkür ederiz. Bu gerekli adımın uyum sorunlarına yol açabileceğini biliyoruz ancak kısa süreli bu sorunlar, müşterilerimizin hesaplarının ve finansal verilerinin güvenliğini koruma sözümüzle karşılaştırıldığında oldukça hafif kalıyor.