Beveiliging voor webwinkels

Systeemupgradegids

Klik HIER voor informatie over SHA-256-naleving.

Maak uw integratie toekomstbestendig

Wereldwijde beveiligingsrisico's veranderen voortdurend en de veiligheid van onze webwinkels blijft onze hoogste prioriteit. Ter bescherming tegen de huidige en toekomstige bedreigingen moedigen we onze webwinkels aan om hun integratie te upgraden door het volgende te doen:

1. Stoppen met het gebruik van het VeriSign G2-basiscertificaat
2. De integratie bijwerken zodat certificaten die het SHA-256-algoritme gebruiken worden ondersteund

Waarom moet ik veranderingen doorvoeren?

De publieke certificeringsinstantie (Certificate Authority, CA) blijft werken aan het verbeteren van de veiligheid van SSL-certificaten. Ter voorbereiding op het vereiste gebruik van het SHA-256-handtekeningalgoritme in 2016 wordt gestopt met de ondersteuning van het VeriSign G2-basiscertificaat dat in het verleden werd gebruikt voor de verbinding met eindpunten van de PayPal-API en IPN (Direct betaalbericht).

Wanneer moet ik actie ondernemen?

We raden u aan om u zo snel mogelijk op deze wijzigingen voor te bereiden. Voor een gedetailleerde planning met de upgradedatums voor Live en Sandbox API-eindpunten raadpleegt u de microsite 2015-2016 SSL Certificate Change.

NOTE: Deze wijzigingen zijn van belang omdat ze dienen om beveiligingsproblemen aan te pakken die voor de gehele industrie gelden en die niet uniek zijn voor PayPal. Door hun implementatie worden de privacy en betrouwbaarheid van uw PayPal-integraties verbeterd. Omdat de details van deze wijzigingen per systeem verschillen, raden we u aan om voor uitvoering de hulp van een gekwalificeerde systeembeheerder in te roepen.

1. Stoppen met het gebruik van het VeriSign G2-basiscertificaat

Het probleem: in het verleden gaf VeriSign SSL-certificaten uit met een vertrouwensketen die was ondertekend door een 1024-bits G2-basiscertificaat. In de afgelopen jaren zijn de overheid en de publieke CA-industrie overgestapt op veiligere 2048-bits certificaten, zodat VeriSign nu SSL-certificaten uitgeeft met een vertrouwensketen die is ondertekend door een in 2006 uitgegeven 2048-bits G5-basiscertificaat.

Onze oplossing: conform industriestandaarden accepteert PayPal niet langer veilige verbindingen met de API/IPN-eindpunten waarbij wordt verwacht dat ons certificaat/onze vertrouwensketen wordt ondertekend door het G2-basiscertificaat. Alleen verzoeken voor een veilige verbinding waarbij wordt verwacht dat ons certificaat/onze vertrouwensketen wordt ondertekend door het G5-basiscertificaat, zullen een veilige verbinding opleveren.

U moet het volgende doen:

Stop met het gebruik van SSL-verbindingen die het VeriSign-basiscertificaat met een G2-referentie gebruiken als uw systeem op dit moment het gebruik van dit specifieke basiscertificaat machtigt. De industrie is actief bezig om 1024-bits basiscertificaten dit jaar af te schaffen.

- Veilige verbindingen die gebruikmaken van onze certificaatketen die wordt ondertekend door een G2-basiscertificaat, worden niet ondersteund:

Organisatie-eenheid	Klasse 3 publieke primaire certificeringsinstantie - **G2**
Serienummer	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Vingerafdruk certificaat SHA-1	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Veilige verbindingen die gebruikmaken van onze certificaatketen die wordt ondertekend door het G5-basiscertificaat worden ondersteund:

Common Name	VeriSign-klasse 3 publieke primaire certificeringsinstantie - **G5**
Serienummer	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Vingerafdruk certificaat SHA-1	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Volg deze richtlijnen om ervoor te zorgen dat u over een veilige verbinding beschikt met behulp van een ondersteund VeriSign G5-basiscertificaat:

1. **Controleer uw certificaatarchief.** Vraag uw websitehost of de systeembeheerder om te controleren of het VeriSign G5-basiscertificaat is opgenomen in het certificaatarchief dat door uw code wordt gebruikt voor de validatielogica. Als dat het geval is, hoeft u geen actie te ondernemen.
    - Controleer via de volgende koppelingen uw sleutelarchief op de aanwezigheid van het G5-basiscertificaat via Java, Linux of Windows.
2. **Controleer uw foutenlogbestanden.** Als het VeriSign G5-basiscertificaat niet is gedownload ter vervanging van het G2-basiscertificaat, ziet u mogelijk foutmeldingen die ongeveer als volgt luiden:
    - SSL-handshakefout, "Geen vertrouwd certificaat gevonden"
    - Resultaatcode -31, "De certificaatketen kon niet worden gevalideerd, geen lokaal certificaat gevonden"
    - Resultaatcode -8, "SSL-verbinding is mislukt"
    - -1 fout

    Om deze problemen op te lossen, voert u een van de volgende handelingen uit:
    - Werk uw software bij naar de meest recente versie die SHA-256 ondersteunt.
    - Als u een sleutelarchief gebruikt voor de validatie/verificatie van certificaten, moet u het VeriSign G5-basiscertificaat in uw sleutelarchief installeren.
3. **Vraag een VeriSign G5-basiscertificaat aan.** Als uw certificaatarchief of Java-client niet het VeriSign G5-basiscertificaat bevat, vraagt u uw systeembeheerder om dit certificaat te downloaden van VeriSign en op te slaan in het certificaatarchief en in eventuele andere verificatiepakketten voor SSL-verbindingen.
    - Download het VeriSign G5-basiscertificaat van Symantec
    - Download specifieke SSL-servercertificaten, als uw server dat vereist

2. Voer een update uit naar het SHA-256-handtekeningalgoritme

Het probleem: SHA-1 is een 22 jaar oud cryptografisch algoritme dat risico's loopt door de toegenomen rekenkracht. SHA-256 gebruikt een krachtiger algoritme met 256-bits hash-waarden.

Onze oplossing: halverwege 2016 gaat PayPal de SSL-certificaten op alle Live- en Sandbox-eindpunten upgraden van SHA-1 naar het sterkere en robuustere SHA-256.

U moet het volgende doen:

Volg deze richtlijnen om van SSL-certificaten die het SHA-1-handtekeningalgoritme gebruiken over te stappen op SSL-certificaten die het sterkere SHA-256-algoritme gebruiken:

1. **Controleer uw omgeving.** Zorg dat uw omgeving SHA-256-certificaten ondersteunt.
   - Raadpleeg online informatie zoals de SHA-2-compatibiliteitshandleiding van DigiCert en de lijst van ondersteunde browsers en servers van Symantec voor een lijst van ondersteunde hardware en software.
   - Als delen van uw omgeving SHA-256 niet ondersteunen, moet u die delen upgraden of vervangen voordat u de nieuwe certificaten kunt implementeren.
   - Windows 2000 Server en sommige versies van Windows XP zijn mogelijk niet compatibel met SHA-2. Deze Windows PKI-blog over SHA-2 en Windows kan u helpen met patches en aanbevelingen voor het upgraden van uw omgeving.
2. **Controleer uw certificaten.** Als uw omgeving SHA-256 ondersteunt, controleert u of uw sleutelarchief het VeriSign G5-basiscertificaat bevat.

Heeft u vragen?

Raadpleeg voor aanvullende informatie en veelgestelde vragen de microsite 2015-2016 SSL Certificate Change.

Dank u!

Bedankt voor uw aandacht voor dit probleem en uw begrip voor onze aanpak. Hoewel we inzien dat deze noodzakelijke stappen compatibiliteitsproblemen kunnen veroorzaken, kunnen we niet genoeg benadrukken dat deze korte periode van ongemak geenszins opweegt tegen onze gemeenschappelijke belofte aan onze klanten om hun rekeningen en financiële gegevens veilig te bewaren.