Forhandlersikkerhet

Veiledning for systemoppgradering

Klikk HER for informasjon om samsvar med SHA-256.

Fremtidssikring for integrasjonen din

Globale sikkerhetstrusler er i stadig endring, og forhandlernes sikkerhet er vår høyeste prioritet. Vi oppfordrer derfor alle PayPal-forhandlere til å oppgradere integrasjonene sine som følger, for å beskytte dem mot eksisterende og fremtidige trusler:

1. Avslutte bruk av VeriSign G2-rotsertifikatet
2. Oppdatere integrasjonen til å støtte sertifikater som bruker SHA-256-algoritmen

Hvorfor denne endringen?

Den offentlige sertifikatutstedersektoren forbedrer kontinuerlig sikkerheten for SSL-sertifikater. Som et ledd i forberedelsene for krav om bruk av SHA-256-signeringsalgoritmen i 2016, vil VeriSign G2-rotsertifikatet, som har blitt brukt for tilkobling til PayPals API- og varsling om direktebetaling (IPN)-endepunkter, ikke lenger være støttet.

Når må jeg gjøre dette?

Vi anbefaler at du handler så raskt som mulig for å være forberedt på disse endringene. Du finner en detaljert tidslinje, inkludert datoer for oppgraderinger av endepunktene for det publiserte miljøet og Sandbox API, på mikronettstedet for SSL-sertifikatendringer i 2015–2016.

NOTE: Det er viktig å være oppmerksom på at disse endringene er tiltak som skyldes bransjeomfattende sikkerhetsproblemer, og ikke er unike for PayPal. Implementering av endringene vil forbedre personvernet og påliteligheten til PayPal-integrasjonen. Detaljene for disse endringene kan variere fra system til system, derfor anbefaler vi at de utføres ved hjelp av en kvalifisert systemadministrator.

1. Avslutte bruk av VeriSign G2-rotsertifikatet

Problemet: Tidligere utstedte VeriSign SSL-sertifikater som hadde en klareringskjede signert av et 1024-biters G2-rotsertifikat. I de senere årene har myndighetene og den offentlige sertifiseringssektoren gått over til å benytte sikrere 2048-biters sertifikater. VeriSign utsteder derfor nå SSL-sertifikater som har en klareringskjede signert av et 2048-biters G5-rotsertifikat utstedt i 2006.

Vårt tiltak: I samsvar med industristandardene kommer PayPal ikke lenger til å godta sikre tilkoblinger til API/IPN-endepunktene som forventer at sertifikatet/klareringskjeden vår signeres av G2-rotsertifikatet. Kun sikre tilkoblingsforespørsler som forventer at sertifikatet/klareringskjeden vår signeres av G5-rotsertifikatet, vil føre til opprettelse av sikre tilkoblinger.

Gjøremål

Avslutt bruk av SSL-tilkoblinger som avhenger av VeriSign-rotsertifikater med en G2-ID, hvis systemet for øyeblikket krever bruk av dette bestemte rotsertifikatet. Bransjen jobber aktivt med å fase ut 1024-biters rotsertifikatet i løpet av inneværende år.

- Sikre tilkoblinger som avhenger av at sertifikatkjeden vår signeres av G2-rotsertifikatet støttes ikke:

Organisatorisk enhet	Offentlig, primær sertifiseringsinstans i klasse 3 – **G2**
Serienummer	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Fingeravtrykk for SHA1-sertifikat	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Sikre tilkoblinger som avhenger av at sertifikatkjeden vår signeres av G5-rotsertifikatet, støttes:

Vanlig navn	VeriSign offentlig, primær sertifiseringsinstans i klasse 3 – **G5**
Serienummer	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Fingeravtrykk for SHA1-sertifikat	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Følg disse retningslinjene for å sikre at du har en sikker tilkobling som bruker et støttet VeriSign G5-rotsertifikat:

1. **Sjekk sertifikatlageret.** Be verten for nettstedet eller systemadministratoren om å bekrefte at VeriSign G5-rotsertifikatet finnes i rotlageret som koden bruker for valideringslogikk. Hvis dette er tilfellet, må du ikke gjøre noe.
   - Se de følgende koblingene for å sjekke at et G5-rotsertifikat som bruker Java, Linux eller Windows finnes i KeyStore.
2. **Sjekk feilloggene.** Hvis VeriSign G5-rotsertifikatet ikke har blitt lastet ned for å erstatte G2-rotsertifikatet, kan du se feilmeldinger som disse:
   - SSL-håndtrykksfeil, 'No trusted certificate found'
   - Resultatkode -31, 'The certificate chain did not validate, no local certificate found'
   - Resultatkode -8: 'SSL connection faile'
   - -1-feil

   Gjør ett av det følgende for å løse disse problemene:
   - Oppdater programvaren til den nyeste versjonen som støtter SHA-256.
   - Hvis KeyStore brukes til sertifikatvalidering/-godkjenning, installer VeriSign G5-rotssertifikatet i KeyStore.
3. **Hent et VeriSign G5-rotsertifikat.** Hvis sertifikatlageret eller Java-klienten ikke inneholder VeriSign G5-rotsertifikatet, kan du be systemadministratoren om å laste det ned fra VeriSign og lagre det i sertifikatlageret samt alle andre pakker for godkjenning av SSL-tilkobling.
   - Last ned Symantecs VeriSign G5-rotsertifikat
   - Last ned serverspesifikke SSL-sertifikater hvis serveren din krever dette.

2. Oppdater til SHA-256-signeringsalgoritmen

Problemet: SHA-1 er en 22 år gammel kryptografisk algoritme som har problemer med å holde takt med den økte databehandlingskraften. SHA-256 bruker en sterkere algoritme med 256-biters hash-kodeverdier.

Vårt tiltak: PayPal oppgraderer SSL-sertifikatene på alle endepunkter for det publiserte miljøet og Sandbox fra SHA-1 til det sterkere og mer robuste SHA-256 i midten av 2016.

Gjøremål

Følg veiledningen for å gå over fra SSL-sertifikater som benytter SHA-1-signeringsalgoritme, til den sterkere SHA-256-signeringsalgoritmen:

1. **Sjekk miljøet.** Påse at miljøet ditt støtter SHA-256-sertifikater.
   - Hvis du ønsker å se en liste over maskin- og programvare som støttes, kan du se ressurser på Internett, f.eks. DigiCerts veiledning om SHA-2-kompatibilitet og Symantecs liste over støttede nettlesere og servere.
   - Hvis deler av miljøet ikke støtter SHA-256, må du erstatte eller oppgradere disse delene før du kan implementere de nye sertifikatene.
   - Windows 2000 Server og noen versjoner av Windows XP kan være inkompatible med SHA-2. Denne Windows PKI-bloggen om SHA2 og Windows kan hjelpe med nødvendige oppdateringer og anbefalinger for å oppgradere miljøet.
2. **Sjekk sertifikatene.** Hvis miljøet ditt støtter SHA-256, må du påse at VeriSign G5-rotsertifikatet finnes i nøkkellageret.

Har du spørsmål?

Hvis du vil ha mer informasjon eller lese svar på vanlige spørsmål, kan du se mikronettstedet for SSL-sertifikatendringer i 2015–2016.

Takk

Takk for at du tar tak i dette problemet raskt. Vi forstår at dette kan føre til kompatibilitetsproblemer på kort sikt, men vi kan ikke få understreket nok at denne kortvarige uleiligheten er noe vi må gjennom for at vi skal kunne sørge for at kontoene og betalingsopplysningene til våre respektive kunder er sikre.