Sicurezza

Guida all'aggiornamento del Sistema

Clicca QUI per informazioni sulla conformità allo standard SHA-256.

Ottimizza la tua integrazione

In un mondo in cui le minacce alla sicurezza mutano costantemente, la nostra priorità numero uno è mantenere i nostri utenti al sicuro. Per proteggerti da minacce presenti e future, ti invitiamo a eseguire i seguenti aggiornamenti alla tua integrazione:

1. Interrompere l'uso del VeriSign G2 Root Certificate
2. Aggiornare l'integrazione per supportare i certificati che usano l'algoritmo SHA-256

Perché cambiare?

Le Certificate Authority (CA) pubbliche apportano regolari miglioramenti alla sicurezza dei certificati SSL. In vista dell'utilizzo obbligatorio dell'algoritmo SHA-256 previsto per il 2016, il VeriSign G2 Root Certificate, da sempre usato per la connessione agli endpoint API e Notifica immediata di pagamento (IPN) di PayPal, non sarà più supportato.

Quando eseguire le operazioni consigliate?

Si consiglia di agire al più presto per prepararsi a questi cambiamenti. Per conoscere le tempistiche esatte, tra cui le date di aggiornamento degli endpoint API Sandbox, visita il 2015-2016 SSL Certificate Change Microsite.

NOTE: È importante notare che queste modifiche mirano a risolvere i problemi di sicurezza di tutto il settore, non solo di PayPal. Una volta implementate, miglioreranno la privacy e l'affidabilità delle integrazioni di PayPal. Poiché i dettagli delle modifiche variano in base al sistema, ti consigliamo di eseguirle con l'assistenza di un amministratore di sistema qualificato.

1. Interruzione dell'uso del VeriSign G2 Root Certificate

Il problema: in passato, VeriSign rese disponibili certificati SSL con una catena di attendibilità convalidata da un G2 Root Certificate a 1024 bit. In anni più recenti, le Certificate Authority pubbliche hanno optato per certificati più sicuri a 2048 bit; pertanto VeriSign ora emette certificati SSL con una catena di attendibilità convalidata da un G5 Root Certificate a 2048 bit, emesso nel 2006.

La nostra risposta: in conformità agli standard di settore, PayPal NON accetterà più connessioni agli endpoint API/IPN che prevedano la convalida del certificato o della catena di attendibilità effettuata mediante G2 Root Certificate. Si garantiscono connessioni sicure solo in caso di richieste di connessione protetta da certificato o catena di attendibilità convalidati da G5 Root Certificate.

Cosa devi fare…

Non usare più connessioni SSL protette da VeriSign G2 Root Certificate, se il sistema in uso richiede questo specifico certificato. Il settore si sta adoperando attivamente per eliminare i Root Certificate a 1024 bit entro quest'anno.

- Le connessioni protette mediante la nostra catena di certificati convalidata dal G2 Root Certificate non sono supportate:

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

- Le connessioni protette mediante la nostra catena di certificati convalidata dal G5 Root Certificate sono supportate:

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

Segui queste linee guida per assicurarti di essere connesso in modo protetto mediante un VeriSign G5 Root Certificate:

1. **Controlla l'archivio dei certificati.** Chiedi all'host del tuo sito o all'amministratore del sistema di verificare che il VeriSign G5 Root Certificate sia incluso nell'archivio dei certificati radice usato dal codice per la logica di convalida. Se già rispetti questi requisiti, non devi intraprendere alcuna azione.
    - Clicca i link di seguito per verificare che nel tuo keystore sia presente il G5 Root Certificate che utilizza Java, Linux o Windows.
2. **Controlla i Registri errori.** Se il VeriSign G5 Root Certificate non è stato scaricato per sostituire il G2 Root Certificate, potrebbero comparire messaggi di errore simili a quelli riportati di seguito:
    - Errore handshake SSL, “No trusted certificate found”
    - Codice risultato -31, “The certificate chain did not validate, no local certificate found”
    - Codice risultato -8, “SSL connection failed”
    - Errore -1

    Per risolvere questi problemi, procedi in uno dei seguenti modi:
    - Aggiorna il software alla versione più recente che supporti SHA-256.
    - Se viene usato un keystore per la convalida/autenticazione del certificato, installa il VeriSign G5 Root Certificate nel keystore.
3. **Ottieni un VeriSign G5 Root Certificate.** Se il tuo archivio certificati o il client Java non include il VeriSign G5 Root Certificate, chiedi all'amministratore del sistema di scaricarlo da VeriSign e salvarlo nell'archivio dei certificati, insieme ad altri eventuali pacchetti di autenticazione della connessione SSL.
    - Scarica il VeriSign G5 Root Certificate di Symantec
    - Scarica certificati SSL server specifici, se richiesti dal server

2. Aggiorna il sistema all'algoritmo SHA-256

Il problema: SHA-1 è un algoritmo crittografico creato 22 anni fa, e oggi è minacciato dall'aumento della potenza di elaborazione. SHA-256 usa un algoritmo più sicuro con valori hash a 256 bit.

La nostra risposta: a metà 2016, PayPal aggiornerà i certificati SSL su tutti gli endpoint Live e Sandbox da SHA-1 a SHA-256, più sicuro e affidabile.

Cosa devi fare…

Segui le istruzioni riportate di seguito per passare dai certificati SSL che usano l'algoritmo di accesso SHA-1 a quelli che usano l'algoritmo di accesso SHA-256 più sicuro:

1. **Controlla l'ambiente.** Assicurati che il tuo ambiente supporti i certificati SHA-256.
   - Consulta le risorse online, ad esempio la guida DigiCert's SHA-2 Compatibility Guide e l'elenco Symantec's Supported Browser and Server List, per conoscere gli hardware e i software supportati.
   - Se alcune parti del tuo ambiente non supportano SHA-256, sostituisci o modifica queste parti prima di implementare i nuovi certificati.
   - Windows 2000 Server e alcune versioni di Windows XP potrebbero non essere compatibili con SHA-2. Il blog Windows PKI blog on SHA2 and Windows fornisce assistenza offrendo patch e consigli utili per l'aggiornamento dell'ambiente.
2. **Controlla i tuoi certificati.** Se il tuo ambiente supporta SHA-256, accertati di avere il VeriSign G5 Root Certificate nel tuo keystore.

Hai altre domande?

Per maggiori informazioni e per consultare le domande frequenti, visita il 2015-2016 SSL Certificate Change Microsite.

Grazie.

Ti ringraziamo per l'attenzione. Benché consapevoli che le operazioni richieste potrebbero provocare problemi di compatibilità, tale disagio sarà ricompensato dal fatto che i conti e i dati finanziari dei nostri e dei tuoi clienti saranno al sicuro.