Bezpieczeństwo handlowców

Przewodnik dotyczący uaktualnienia system

Kliknij tutaj aby uzyskać informacje na SHA-256.

Przygotowanie integracji do przyszłych zmian

Globalne zagrożenia dla bezpieczeństwa stale się zmieniają, a bezpieczeństwo naszych handlowców ma dla nas wciąż najwyższy priorytet. Aby się zabezpieczyć przed obecnymi i przyszłymi zagrożeniami, zachęcamy naszych handlowców do wprowadzenia w ich integracjach następujących uaktualnień:

1. Należy zaprzestać korzystania z certyfikatu głównego VeriSign G2.
2. Należy uaktualnić integrację w taki sposób, aby obsługiwała certyfikaty z wykorzystaniem algorytmu SHA-256.

Dlaczego należy wprowadzić te zmiany?

Branża publicznych urzędów certyfikacji (ang. Certificate Authority, CA) konsekwentnie podnosi poziom bezpieczeństwa certyfikatów SSL. W ramach przygotowań do wprowadzenia w roku 2016 wymogu korzystania z algorytmu podpisu SHA-256 zaprzestanie się obsługi certyfikatu głównego VeriSign G2 wykorzystywanego w przeszłości do nawiązywania połączeń z punktami końcowymi PayPal API i BPP (Błyskawiczne powiadamianie o płatności).

Kiedy należy podjąć działania?

Szczegółowy harmonogram, w tym daty uaktualniania dla punktów końcowych API aktywnej witryny PayPal i środowiska Sandbox, można znaleźć na mikrostronie dotyczącej zmian w certyfikatach SSL wprowadzanych w latach 2015-2016.

NOTE: Należy zauważyć, że zmiany te mają doprowadzić do rozwiązania problemów z bezpieczeństwem występujących w całej branży i będą wdrażane nie tylko w systemie PayPal. Ich wdrożenie przyczyni się do zwiększenia poufności i niezawodności Państwa integracji PayPal. Szczegóły tych zmian zależą od systemu, zalecamy więc, aby je wprowadzać z pomocą wykwalifikowanego administratora systemu.

1. Zaprzestań korzystania z certyfikatu głównego VeriSign G2

Problem: W przeszłości firma VeriSign wydawała certyfikaty SSL z łańcuchem zaufania podpisanym z wykorzystaniem 1024-bitowego certyfikatu głównego G2. W ostatnich latach administracja publiczna i branża publicznych urzędów certyfikacji przeszła na bezpieczniejsze certyfikaty 2048-bitowe, w wyniku czego firma VeriSign wydaje teraz certyfikaty SSL z łańcuchem zaufania podpisanym z wykorzystaniem 2048-bitowego certyfikatu głównego G5 wystawionego w 2006 r.

Reakcja firmy PayPal: Zgodnie ze standardami branżowymi PayPal zaprzestanie akceptowania bezpiecznych połączeń z punktami końcowymi API/BPP, które oczekują podpisywania naszego łańcucha certyfikatów lub łańcucha zaufania za pomocą certyfikatu głównego G2. Do udanego nawiązania bezpiecznych połączeń doprowadzą jedynie te żądania takich połączeń, które oczekują podpisywania naszego łańcucha certyfikatów lub łańcucha zaufania za pomocą certyfikatu głównego G5.

Co należy teraz zrobić?

Zaprzestań korzystania z połączeń SSL opartych na certyfikatach głównych VeriSign z identyfikatorem G2, jeśli Twój obecny system dopuszcza korzystanie z tego konkretnego certyfikatu głównego. Branża dokłada wszelkich starań, aby wycofać 1024-bitowe certyfikaty główne z użytku jeszcze w tym roku.

- Bezpieczne połączenia, które oczekują podpisywania naszego łańcucha certyfikatów za pomocą certyfikatu głównego G2 nie są obsługiwane:

Jednostka organizacyjna	Class 3 Public Primary Certification Authority – **G2**
Numer seryjny	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Odcisk certyfikatu SHA1	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Bezpieczne połączenia, które oczekują podpisywania naszego łańcucha certyfikatów za pomocą certyfikatu głównego G5 są obsługiwane:

Pełna nazwa domeny (ang. Common Name)	VeriSign Class 3 Public Primary Certification Authority – **G5**
Numer seryjny	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Odcisk certyfikatu SHA1	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Postępuj zgodnie z tymi wytycznymi, aby zapewnić nawiązywanie bezpiecznych połączeń z wykorzystaniem obsługiwanego certyfikatu głównego VeriSign G5:

1. **Sprawdź swój magazyn certyfikatów.** Poproś usługodawcę hostującego Twoją witrynę lub administratora systemu o sprawdzenie, czy certyfikat główny VeriSign G5 znajduje się w magazynie głównym wykorzystywanym przez Twój kod do przeprowadzania walidacji. Jeśli tak jest, nie są wymagane żadne działania.
    - Odwiedź strony, do których prowadzą następujące łącza, aby sprawdzić z wykorzystaniem platformy Java, Linux lub Windows, czy w Twoim magazynie kluczy znajduje się certyfikat główny G5.
2. **Sprawdź swoje dzienniki błędów.** Jeśli nie pobrano certyfikatu głównego VeriSign G5, aby zastąpić nim certyfikat główny G2, w dziennikach tych mogą się pojawić komunikaty o błędach podobne do wyświetlonych poniżej:
    - Błąd dotyczący zgodności certyfikatu SSL, „Nie znaleziono zaufanego certyfikatu”
    - Kod wyniku -31, „Nie udało się zatwierdzić łańcucha certyfikatów, nie znaleziono lokalnego certyfikatu”
    - Kod wyniku -8, „Próba połączenia SSL nieudana”
    - Błąd -1

    Aby rozwiązać te problemy, należy wykonać jedną z poniższych czynności:

    - Zaktualizuj oprogramowanie do najnowszej wersji, która obsługuje certyfikat SHA-256.
    - Jeśli do zatwierdzania lub uwierzytelniania certyfikatów jest wykorzystywany magazyn kluczy, zainstaluj w tym magazynie certyfikat główny VeriSign G5.
3. **Uzyskaj certyfikat główny VeriSign G5.** Jeśli Twój magazyn certyfikatów lub klient platformy Java nie zawiera certyfikatu głównego VeriSign G5, poproś administratora swojego systemu o pobranie tego certyfikatu z witryny firmy VeriSign i zapisz go w magazynie certyfikatów. Podobnie w przypadku innych pakietów do uwierzytelniania połączeń SSL.
    - Pobierz certyfikat główny VeriSign G5 firmy Symantec
    - Pobierz specyficzne certyfikaty SSL wymagane przez Twój serwer

2. Zaktualizuj algorytm podpisu do wersji SHA-256

Problem: SHA-1 to algorytm szyfrowania stosowany od 22 lat, który z uwagi na wzrost mocy obliczeniowej komputerów przestaje już wystarczać. W algorytmie SHA-256 zastosowano silniejszy mechanizm korzystający z 256-bitowych wartości mieszających.

Reakcja firmy PayPal: PayPal uaktualnia certyfikaty SSL we wszystkich punktach końcowych aktywnej witryny PayPal i środowiska Sandbox, planując przejść do połowy 2016 r. z algorytmu SHA-1 na silniejszy i bardziej zaawansowany algorytm SHA-256.

Co należy teraz zrobić?

Postępuj zgodnie z niniejszymi wytycznymi dotyczącymi przejścia z certyfikatów SSL wykorzystujących algorytm podpisu SHA-1 na silniejszy algorytm SHA-256.

1. **Sprawdź swoje środowisko.** Zadbaj o to, aby środowisko obsługiwało certyfikaty SHA-256.
   - Listę obsługiwanego sprzętu i oprogramowania znajdziesz w materiałach dostępnych online, takich jak Przewodnik firmy DigiCert dotyczący zgodności ze standardem SHA-2 oraz lista przeglądarek i serwerów obsługiwanych przez firmę Symantec.
   - Jeśli elementy Twojego środowiska nie obsługują algorytmu SHA-256, przed wdrożeniem nowych certyfikatów trzeba te elementy wymienić lub uaktualnić.
   - System Windows 2000 Server i niektóre wersje systemu Windows XP mogą być niezgodne ze standardem SHA-2. Ten blog poświęcony infrastrukturze klucza publicznego (PKI) w systemie Windows, w którym porusza się kwestie standardu SHA-2 i systemu Windows, może pomóc w dotarciu do łatek i zaleceń dotyczących uaktualnienia środowiska.
2. **Sprawdź swoje certyfikaty.** Jeśli Twoje środowisko obsługuje algorytm SHA-256, upewnij się, że masz w swoim magazynie kluczy certyfikat główny VeriSign G5.

Masz pytania?

Dodatkowe informacje i często zadawane pytania można znaleźć na mikrostronie dotyczącej zmian w certyfikatach SSL wprowadzanych w latach 2015-2016.

Dziękujemy!

Dziękujemy za szybką reakcję w tej sprawie i zrozumienie dla wprowadzonych przez nas zmian. Zdajemy sobie sprawę, że te niezbędne kroki mogą prowadzić do problemów ze zgodnością, ale dzięki nim zapewnimy pełne bezpieczeństwo kont i danych finansowych naszych klientów.