Безопасность в системе –

Руководство по обновлению системы для продавцов

Щелкните ЗДЕСЬ, чтобы получить информацию о соответствии требованиям стандарта SHA-256.

Интеграция, соответствующая требованиям будущего

Глобальные угрозы безопасности постоянно меняются, и безопасность наших продавцов по-прежнему имеет для нас первостепенную важность. Чтобы обеспечить защиту от текущих и будущих угроз, мы рекомендуем нашим продавцам обновлять свою интеграцию следующим образом:

1. Не используйте корневой сертификат VeriSign G2.
2. Обновите интеграцию для поддержки сертификатов с использованием алгоритма шифрования SHA-256.

Для чего необходимы эти изменения

Государственные сертифицирующие органы постоянно улучшают уровень безопасности сертификатов SSL. В рамках подготовки к требованию использовать алгоритм подписи SHA-256 в 2016 году больше не будет поддерживаться корневой сертификат VeriSign G2, который ранее использовался для соединения с API-интерфейсом PayPal и конечными точками мгновенного уведомления о платежах (IPN).

Когда пора действовать

Мы рекомендуем Вам принять незамедлительные меры, чтобы подготовиться к этим изменениям. Для ознакомления с подробным графиком, в том числе с датами обновления конечных точек API-интерфейса в изолированной и продуктивной программной среде, см. микросайт по изменению сертификатов SSL в 2015–2016 гг.

NOTE: Важно обратить внимание на то, что эти изменения относятся ко общеотраслевым проблемам безопасности и не уникальны для PayPal. Их реализация улучшит конфиденциальность и надежность вашей интеграции PayPal. Поскольку конкретные свойства этих изменений варьируются в зависимости от системы, рекомендуется доверить их внедрение квалифицированному системному администратору.

1. Прекратить использование корневого сертификата VeriSign G2

Проблема. Ранее компанией VeriSign были выпущены SSL-сертификаты, у которых была доверительная цепочка, подписанная 1024-разрядным корневым сертификатом G2. В последние годы государственные сертифицирующие органы перешли на использование более безопасных 2048-разрядных сертификатов. Таким образом, VeriSign в данный момент выпускает SSL-сертификаты с доверительной цепочкой, подписанной 2048-разрядным корневым сертификатом G5, выпущенным в 2006 году.

Наше решение. В соответствии с отраслевыми стандартами PayPal больше не принимает безопасные соединения к конечным точкам API-интерфейса или мгновенного уведомления о платежах, которые ожидают подписания нашего сертификата или доверительной цепочки корневым сертификатом G2. Только запросы безопасного соединения, ожидающие подписания сертификата или доверительной цепочки корневым сертификатом G5, приведут к успешным безопасным соединениям.

Что необходимо сделать

Прекратите использование SSL-соединений, которые основываются на корневых сертификатах VeriSign с идентификатором G2, если ваша система в настоящее время настроена на использование этого корневого сертификата. Компании нашей отрасли активно работают, чтобы постепенно сократить использование 1024-разрядных корневых сертификатов в этом году.

- Не поддерживаются безопасные соединения, которые основываются на нашей цепочке сертификата, подписываемой корневым сертификатом G2:

Организационная единица	Class 3 Public Primary Certification Authority — **G2**
Серийный номер	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Цифровой отпечаток сертификата SHA1	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Поддерживаются безопасные соединения, которые основываются на нашей цепочке сертификата, подписываемой корневым сертификатом G5:

Общее название	VeriSign Class 3 Public Primary Certification Authority — **G5**
Серийный номер	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Цифровой отпечаток сертификата SHA1	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Следуйте этим инструкциям, чтобы проверить надежность соединения с использованием поддерживаемого корневого сертификата VeriSign G5:

1. **Проверьте свое хранилище сертификатов.** Попросите хост вашего веб-сайта или своего системного администратора проверить, что корневой сертификат VeriSign G5 включен в корневое хранилище, которое используется вашим кодом для логики проверки. Если так, никаких дальнейших действий не требуется.
    - Посмотрите следующие ссылки, чтобы проверить ваше хранилище ключей на наличие корневого сертификата G5, используя Java, Linux или Windows.

2. **Проверьте свои журналы ошибок.** Если корневой сертификат VeriSign G5 не был загружен для замены корневого сертификата G2, вы можете получить сообщения об ошибках, например:

   - Ошибка квитирования SSL, «Доверяемый сертификат не найден».
   - Код результата –31, «Нет подтверждения цепочки сертификата, локальный сертификат не найден».
   - Код результата –8, «Прервана связь SSL».
   - Ошибка –1.

   Для решения этих проблем выполните одно из следующих действий:

   - Обновите свое программное обеспечение до последней версии, которая поддерживает SHA-256.
   - Если хранилище ключей используется для проверки или подтверждения сертификата, установите корневой сертификат VeriSign G5 в свое хранилище ключей.

3. **Получите корневой сертификат VeriSign G5.** Если ваше хранилище сертификатов или клиент Java не включают корневой сертификат VeriSign G5, то попросите своего системного администратора загрузить его с VeriSign и сохранить в хранилище сертификатов, а также любых других пакетах подтверждения соединения SSL.

   - Загрузите корневой сертификат VeriSign G5 Symantec.
   - Загрузите специальные SSL-сертификаты сервера, если это необходимо для вашего сервера.

2. Установить обновление до алгоритма подписания SHA-256

Проблема. SHA-1 — это криптографический алгоритм, созданный 22 года назад, которому угрожают увеличения вычислительной мощности. SHA-256 использует более сильный алгоритм с 256-разрядными значениями хэш-функции.

Наше решение. PayPal обновит SSL-сертификаты на всех конечных точках и конечных точках продуктивной и изолированной программной среды с версии SHA-1 на более сильную и устойчивую SHA-256 в середине 2016 года.

Что необходимо сделать

Следуйте этим инструкциям, чтобы перейти от использования SSL-сертификатов, которые используют алгоритм подписания SHA-1 к более сильному алгоритму подписания SHA-256:

1. **Проверьте свою среду.** Убедитесь в том, что ваша среда поддерживает сертификаты SHA-256.

   - Обратитесь к интернет-ресурсам, таким как Руководство по совместимости SHA-2 от DigiCert и список поддерживаемых браузеров и серверов от Symantec, чтобы ознакомиться с перечнем поддерживаемого оборудования и программного обеспечения.
   - Если части вашей среды не поддерживают SHA-256, вам необходимо заменить или обновить эти части, прежде чем вы сможете внедрить новые сертификаты.
   - Windows 2000 Server и некоторые версии Windows XP могут быть несовместимыми с SHA-2. Этот блог Windows PKI о SHA2 и Windows может помочь с патчами и рекомендациями по обновлению вашей среды.

2. **Проверьте свои сертификаты.** Если ваша среда поддерживает SHA-256, убедитесь в наличии корневого сертификата VeriSign G5 в вашем хранилище ключей.

У вас остались вопросы?

Подробности и часто задаваемые вопросы доступны на микросайте [2015-2016 SSL Certificate change]

Спасибо!

Благодарим вас за то, что вы проявили внимание к этой проблеме и разделяете наш подход к ее решению. Мы понимаем, что эти обязательные меры могут вызвать проблемы с совместимостью. Однако мы хотели бы подчеркнуть, что это временное неудобство в большой степени компенсируется нашим обещанием обеспечить безопасность счетов и финансовых сведений наших общих клиентов.