

## Типовые проблемы SSL при прохождении ASV-сканирования

05.07.2009

*Множество попыток пройти ASV-сканирование завершаются неудачно по причине некорректной настройки SSL. В статье описаны типовые проблемы, связанные с использованием SSL и приведены рекомендации по их устранению.*

*Александр Поляков, ведущий аудитор информационной безопасности компании Digital Security*

В ходе анализа отчётов ASV сканирований практически на каждом хосте обнаруживается ряд уязвимостей, которые не позволяют получить сертификат соответствия. Довольно часто хост, который с первого взгляда кажется защищённым и не содержит явных уязвимостей, не проходит ASV сканирование из-за небезопасных настроек SSL шифрования, которые могут привести к проблемам различных уровней критичности. Недостаточно просто включить SSL шифрование. Не менее важно безопасно его настроить, что позволит не только соответствовать требованию 4.1.a стандарта PCI DSS, но и успешно пройти ASV сканирование.

Ниже приведены основные проблемы с SSL, которые не позволяют пройти ASV сканирование.

№	Уязвимость	Угроза	Критичность уязвимости
1	SSL сервер позволяет анонимную аутентификацию	Атака Man In The Middle	Critical
2	Поддержка короткой длины ключа алгоритма шифрования	Расшифровка трафика	High
3	Уязвимости алгоритма шифрования SSLv2	Атака Man In The Middle	
4	Коллизия алгоритма MD5 при использовании X.509 сертификатов	Фишинг-атака	
5	Использование самоподписанных сертификатов	Создания поддельного WEB-сервера и атака Man In The Middle	Medium

Кроме того, в документе PCI DSS - Technical and Operational Requirements for Approved Scanning Vendors (ASVs) отдельно отмечается, что использование SSLv2 недопустимо: "A component must be considered non-compliant if the installed SSL version is limited to version 2.0, or older. SSL must be a more recent version than 2.0."

Итак, при наличии хотя бы одной из перечисленных уязвимостей сканирование считается не пройденным. Но, несмотря на значительное количество проблем, описанных выше, они могут быть устранены при использовании следующих несложных рекомендаций:

### **Безопасная конфигурация для Web-сервера Apache**

1. Поддержка только протоколов SSLv3 и TLSv1:

SSLProtocol -ALL +SSLv3 +TLSv1

2. Использование ключей длиной не менее 128 бит, запрет анонимного подключения, использование безопасного шифрования.

SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

3. Использование официально подписанных сертификатов.

### **Безопасная конфигурация для Web-сервера IIS**

1. <http://technet.microsoft.com/en-us/library/cc755203.aspx>

2. Использование официально подписанных сертификатов.

Для того чтобы проверить, существуют ли у вас перечисленные уязвимости, можно воспользоваться командами, приведёнными в документе:

<http://pcianswers.com/2007/04/03/pci-diy-checking-for-weak-ssl-encryption-with-openssl/>

Подробное описание настроек SSL для веб-сервера Apache:

[http://livedocs.adobe.com/fms/2/docs/wwhelp/wwhimpl/common/html/wwhelp.htm?context=LiveDocs\\_Parts&file=00000300.html](http://livedocs.adobe.com/fms/2/docs/wwhelp/wwhimpl/common/html/wwhelp.htm?context=LiveDocs_Parts&file=00000300.html)

Подробное описание настроек SSL для веб-сервера IIS:

<http://technet.microsoft.com/en-us/library/cc755203.aspx>

## Об авторе

Александр Поляков – ведущий аудитор информационной безопасности компании Digital Security, специализируется на анализе безопасности бизнес-приложений и систем управления базами данных. Автор книги «Безопасность Oracle глазами аудитора: нападение и защита».

## О стандарте PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) предназначен для обеспечения безопасности обработки, хранения и передачи данных о держателях платежных карт в информационных системах компаний, работающих с международными платежными системами Visa, MasterCard и другими. Стандарт разработан сообществом PCI Security Standards Council, в которое входят мировые лидеры на рынке платежных карт, такие как American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International.

Под действие требований стандарта попадают банки, процессинговые центры, поставщики ИТ-услуг, торгово-сервисные предприятия, и иные организации, обрабатывающие транзакции по международным платежным картам. К части этих компаний международные платежные системы предъявляют требование о прохождении обязательного ежегодного аудита компанией, обладающей статусом QSA.

Текущая версия стандарта 1.2 выпущена 1 октября 2008 года.