Форма нотификации

Зарегистрировано в реестре "02" ноября 2016 № RU00000 28648

М.П.

(Подпись лица уполномоченного органа) В.Н. МАРТЫНОВ (Ф.И.О.)

НОТИФИКАЦИЯ
о характеристиках товара, содержащего шифровальные (криптографические) средства

1. Наименование товара: Программно-аппаратная ленточная библиотека Quantum Scalar Automated Storage Tape Library модель i3 и модель i6, включая запасные части и компоненты. Продукт включает контрольный модуль control module, а также опциональные расширительные модули с ленточными драйверами типа IBM LTO-6 и/или IBM LTO-7, которые могут устанавливаться по требованию пользователей. Описание моделей и парт-номеров (артикулов) продукта:
   1) Модель Quantum Scalar i3 Storage Tape Library идентифицируется по номерам: LSC33-A, LSC3A-A, LSC33-B, LSC33-C, а также по парт-номеру (артикулу) в формате: 9-04;
   2) Модель Quantum Scalar i6 Storage Tape Library идентифицируется по номерам: LSC36, LSC36-A, LSC36-C, а также по парт-номеру (артикулу) в формате: 9-05.

   [встроенное программное обеспечение управления ленточными библиотеками Library Management and Control Software/Firmware (aka Quantum iLayer™) версия 100 - 900]

2. Назначение товара (продукции): Программно-аппаратная ленточная библиотека модель Quantum Scalar i3 Automated Storage Tape Library и модель Quantum Scalar i6 Automated Storage Tape Library представляют собой автоматизированные ленточные библиотеки, обеспечивающие максимально высокую плотность хранения данных с минимально возможным уровнем энергопотребления и уровнем охлаждения, предназначены значительно снизить операционные расходы дата-центров.

   Продукт включает встроенное программное обеспечение управления ленточными библиотеками Library Management and Control Software/Firmware (aka Quantum iLayer™) далее - "встроенное программное обеспечение управления и контроля ленточной библиотекой" или "library control firmware") версия 100 - 900, которое использует криптографические функции публично доступной библиотеки LibreSSL Open Source Software (OSS) (http://www.libressl.org, для безопасного доступа к библиотеке и каналу управления посредством SSL и TLS соединений), а также публичного сетевого протокола аутентификации Kerberos версия 5 релиз 1.14.1 (http://web.mit.edu/Kerberos/krb5-1.14/). Криптографические функции встроенного программного обеспечения управления и контроля ленточной библиотекой (library control firmware) предназначены исключительно для целей аутентификации в виде использования пароля и электронной цифровой подписи (ЭЦП), а также удаленного управления ленточными библиотеками. Встроенное программное обеспечение управления библиотекой не реализует каких-либо дополнительных криптографических функций, которые включали бы проприетарные криптографические функции, а также функции по шифрованию данных при осуществлении управления конфигурацией ленточной библиотекой и иными контрольными функциями.

3. Сведения об изготовителе товара: Квантум Корпорейшн, 224 Аэропорт Парквэй, Сьют 300, Сан Хосе, Калифорния 95110, США, тел. +1 408-944-4000, электронная почта: Mary.Vigil@Quantum.com, официальный сайт в Интернет: http://www.quantum.com (Quantum Corporation, 224 Airport Parkway, Suite 300, San Jose, CA 95110, USA, tel. +1 408-944-4000, e-mail: Mary.Vigil@Quantum.com web-site: http://www.quantum.com).

4. Используемые криптографические алгоритмы (функции): № категории из приложения № 4

Шифровальные функции встроенного программного обеспечения управления и контроля ленточными библиотеками Library Management and Control Software/Firmware (aka Quantum iLayer™) версия 100 - 900:

а) Алгоритмы шифрования и дайджест сообщения алгоритмов, таких как MD2, MD5 (максимальная длина хэша 128 бит), MDC2 (максимальная длина хэша 1024 бит) и SHA (максимальная длина хэша 512 бит), которые используются для электронной цифровой подписи (ЭЦП), проверки целостности библиотеки встроенного программного обеспечения управления, и проверки подлинности доступа и защиты пароля. — 2(1), 2(2), 10

б) Протоколы реализации SSL/TLS публично доступной библиотеки LibreSSL Open Source Software library поддерживают следующие симметричные криптографические алгоритмы для целей безопасного удаленного доступа к продукту: — 2(1), 2(2), 10

- Blowfish, максимальная длина ключа 128 бит
- DES, максимальная длина ключа 56 бит
- 3DES, максимальная длина ключа 56 бит
- Rc2, максимальная длина ключа 64 бит
- Rc4, максимальная длина ключа 128 бит
- AES, максимальная длина ключа 56 бит

в) Протоколы реализации SSL/TLS публично доступной библиотеки LibreSSL Open Source Software library поддерживают следующие асимметричные криптографические алгоритмы для целей безопасного удаленного доступа к продукту: — 2(1), 2(2), 10

- RSA, максимальная длина ключа 4096 бит
- Diffie-Hellman, максимальная длина ключа 512 to 2048 бит
- DSA, максимальная длина ключа 1024 бит

г) Публичный сетевой протокол аутентификации Kerberos версия 5 релиз 1.14.1 поддерживает следующие симметричные криптографические алгоритмы, используемые для целей обеспечения доступа через аутентификацию: — 2(1), 2(2), 10

- DES cbc mode вместе с CRC-32, длина ключа не установлена
- DES cbc mode вместе с RSA-MD4, длина ключа не установлена
- DES cbc mode вместе с RSA-MD5, длина ключа не установлена
- DES вместе с HMAC/sha1, максимальная длина хэша 256 бит DES3 cbc mode вместе с HMAC/sha1, максимальная длина хэша 256 бит
- AES-256 CTS mode вместе с 96-bit SHA-1 HMAC, максимальная длина хэша 256 бит
- AES-128 CTS mode вместе с 96-bit SHA-1 HMAC, максимальная длина хэша 256 бит
- RC4 вместе с HMAC/MD5, максимальная длина хэша 256 бит
- Exportable RC4 вместе с HMAC/MD5, максимальная длина хэша 256 бит

Примечания: 1) Встроенное программное обеспечение управления и контроля ленточной библиотекой не содержит программных интерфейсов для использования шифрования или контроля функциональности или управления ключами, связанными с шифрованием. Параметры работы библиотеки можно настроить только через веб-сервисные интерфейсы (Web-service

interfaces), или использования доступа к файловой системе через логин, где отсутствуют какие-либо функции для манипулирования криптографическими алгоритмами, генерации ключей пользователей или предоставления прямого доступа к шифрованию данных пользователя.

2) Встроенное программное обеспечение управления и контроля ленточными библиотеками Library Management and Control Software/Firmware (aka Quantum iLayerTM) версия 100 - 900 не поддерживает запатентованные методики шифрования, но использует ядро Linux и в целом публично доступные (open source) программные наборы (software packages) с открытым исходным кодом, без изменений, исключительно для защиты логина и пароля, а также защищенной связи и сетевой аутентификации для удаленного управления продуктом.

5. Наличие у товара функциональных возможностей, не описанных в предоставляемой пользователю эксплуатационной документации: нет.

6. Срок действия нотификации: 07.10.2021.

7. Сведения о заявителе: Александр Андреевич Бычков, проживающий по адресу гор. Москва, ул. Короленко д. 8, кв. 73, паспорт 4513 223714 выдан 13.12.2013 Отделением УФМС России по гор. Москве, код подразделения 770-060, тел +7 (495) 787-27-00.

8. Сведения о документе изготовителя, удостоверившего полномочия лица на оформление нотификации (при необходимости): Доверенность, выданная 16 декабря 2013 г. (без номера) компанией Квантум Корпорейшн, 1650 Текнолоджи Драйв, Сьют 700, Сан Хосе, Калифорния 95110, США (Quantum Corporation, 1650 Technology Drive, Suite 700, San Jose, CA 95110, USA), в лице ее Первого вице-президента, главного юридического советника и секретаря Шона Д. Холла гражданину РФ Александру Андреевичу Бычкову, паспорт 4513 223714 выдан 13.12.2013 Отделением УФМС России по гор. Москве, тел +7 (495) 787-27-00.

9. Дата принятия нотификации: 01.11.2016.

Достоверность и полноту сведений, включенных в нотификацию, подтверждаю:

Александр Андреевич Бычков