Форма нотификации

Зарегистрировано в реестре "24" июля 2014 № RU00000 18928

М.П. _____ А.Н.КОВАЛЕВ

(Подпись лица уполномоченного органа) (Ф.И.О.)

НОТИФИКАЦИЯ

О технических характеристиках товаров (продукции),
содержащей криптографические средства

1. Наименование товара (продукции): Масштабируемая ленточная библиотека Quantum Scalar I40/I80 Series с программным обеспечением управления библиотекой library control software/firmware (aka Quantum iLayer™) версия i.6.XX, а также части и компоненты, модель "LSC14-XXXX-XXXX" для серии Scalar I40 и модель "LSC18-XXXX-XXXX" для серии Scalar I80, формат номеров деталей 9-XXXXX-XX.

   При этом символ "X" в описании номера модели, версии программного обеспечения или детали продукта может означать любую цифру от 0 до 9, букву латинского алфавита от A до Z, любой знак или символ, сочетание цифр, букв, знаков или символов, либо их отсутствие.

2. Назначение товара (продукции): Продукт представляет собой сетевое устройство хранения данных (Network Storage Device), включающее в свой состав встроенное программное обеспечение управления библиотекой library control software/firmware (aka Quantum iLayer™) версия i.6.XX, созданное на базе ядра Linux Kernel Module версия 2.6.27-46.

   Магнитно-ленточные накопители для продукта производятся компаниями IBM или HP и поставляются отдельно. В частности, могут использоваться ленточные накопители HP, в отношении которых зарегистрирована нотификация № RU0000012344 (срок действия 31.12.2019), а также IBM, в отношении которых зарегистрирована нотификация № RU0000003175 (модели: 3592-EXX|IBM; 3588-F4A IBM System Storage TS1040; 3588-F5A IBM System Storage TS1050).

   Криптографические функции продукта выполняются на уровне программного обеспечения управления библиотекой library control software/firmware (aka Quantum iLayer™) версия i.6.XX на уровне протоколов SSL, TLS, SSH и Kerberos и ограничены функциями (а) аутентификации в виде защиты пароля, (б) электронно-цифровой подписи и (в) защитой удаленного канала управления продуктом (шифрование траффика данных, а также каких-либо иных криптографических функций продукт не выполняет).

3. Реквизиты производителя товара (продукции): Квантум Корпорейшн, 224 Эйрпорт Парквэй, Сюит 300, Сан Хосе, Калифорния 95110, США, тел. +1 408-944-4000, электронная почта: Mary.Vigil@Quantum.com, официальный веб-сайт в Интернет: http://www.quantum.com, в лице уполномоченного лица Шона Холла, старшего вице-президента и главного юридического советника (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, Shawn Hall – Senior Vice President and General Legal Counsel).

4. Используемые криптографические алгоритмы: № категории товара из приложения 1

Криптографические функции программного обеспечения Quantum iLayer™ версия i.6.XX:

1.1.) Криптографические функции симметричных алгоритмов библиотеки OpenSSL (протоколы SSL, TLS):

- AES-128-cbc, AES-128-ecb длина ключа 128 бит

Александр Анатольевич 2а, 2б, 16 № 77/4352 в Реестре Адвокатов г. Москвы Адвокат

- AES-192-cbc, AES-192-ecb,AES-256-cbc, AES-256-ecb, длина ключа 192 и 256 бит

1.2) Криптографические функции симметричных алгоритмов протокола Kerberos: 2а, 2б, 10

- DES cbc, длина ключа 56 бит, вместе с CRC-32 длина ключа 32 бит
- DES cbc, длина ключа 56 бит, вместе с RSA-MD4, длина ключа не установлена
- DES cbc, длина ключа 56 бит, вместе с RSA-MD5, длина ключа не установлена
- DES, длина ключа 56 бит, вместе с HMAC/sha1, длина хэша 256 бит
- DES3 cbc, длина ключа 168 бит, вместе с HMAC/sha1, длина хэша 256 бит
- AES-256 CTS mode, длина ключа 256 бит, вместе с SHA-1 HMAC, размер хэша 96 бит

1.3) Криптографические функции асимметричных алгоритмов протоколов SSL, TLS (библиотека OpenSSL) и Kerberos: 2а, 2б, 10

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

1.4) Криптографические функции программного модуля LibTomCrypt, разработанного Linux на основе публичных криптографических библиотек (http://libtomcrypt.updatestar.com/ru), используемого в программном компоненте Dropbear версия 20xx-xx, являющегося частью Quantum iLayer™ версия i.6.XX и используемого для поддержки протокола SSH: 2а, 2б, 10

- AES, длина ключа 128 и 256 бит
- Blowfish, длина ключа 128 и 256 бит
- TwoFish, длина ключа 128 и 256 бит
- 3DES, длина ключа 168 бит
- Хэш-функции: SHA1 (размер хэша 160 бит), SHA1_96 (размер хэша 96 бит), SHA2_256 (размер хэша 256 бит), SHA2_512 (размер хэша 512 бит), MD5 (размер хэша 128 бит)

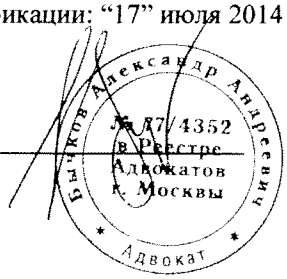
5. Наличие у товара (продукции) функциональных возможностей, не описанных в предоставляемой пользователю эксплуатационной документации: нет.

6. Срок действия нотификации: до 31 декабря 2017 г.

7. Реквизиты заявителя: Александр Андреевич Бычков, адвокат, зарегистрированный в реестре адвокатов г. Москвы под №77/4352, проживающий по адресу гор. Москва, ул. Короленко д. 8, кв. 73, паспорт 45 13 № 223714, выдан 13.12.2013 Отделением УФМС России по гор. Москве по району Сокольники код подразделения 770-060, тел +7 (495) 787-27-00.

8. Реквизиты документа производителя (изготовителя), предоставившего уполномоченному лицу полномочия по оформлению нотификации (при необходимости): Доверенность от 16 декабря 2013 года (без номера), выданная сроком на 3 года 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 адвокату Александру Андреевичу Бычкову, зарегистрированному в реестре адвокатов г. Москвы под №77/4352, тел +7 (495) 787-27-00.

9. Дата принятия нотификации: "17" июля 2014 г.

М.П. 

(Александр Андреевич Бычков)