41066

Зарегистрировано в реестре "15" января 2019 № RU00000 41066

А.В.ПАРФЕНОВ

Для нотификации

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

НОТИФИКАЦИЯ

О технических характеристиках товаров (продукции),
содержащей криптографические средства

1. Наименование товара: Система резервного копирования серии DX*i* Series Disk Based Back up System производства компании Quantum Corporation модели DX*i*90 - DX*i*99, номера моделей DX*i*9000 - DX*i*9999, на базе программного обеспечения Quantum DX*i* Operating Software версии 3 и версии 4 (примечание: каждая подверсия программного обеспечения оканчивается на ".nenc", что означает специальную версию программного обеспечения, адаптированную для РФ/ЕАЭС).

2. Назначение товара: Система резервного копирования серии DXi Series Disk Based Back up System производства компании Quantum Corporation модели DX*i*90 - DX*i*99, номера моделей DX*i*9000 - *DXi*9999, на базе программного обеспечения Quantum DX*i* Operating Software версий 3 и 4 (примечание: каждая подверсия программного обеспечения оканчивается на ".nenc", что означает специальную версию для РФ) предназначена для создания резервных копий важнейшей коммерческой информации, а также для ее хранения восстановления и архивирования. Моделей DX*i*90 - DX*i*99 предназначена для предприятий малого и среднего уровня, максимальный объем хранения и обработки данных составляет от 5 до 135Тб, объем одного жесткого диска от 2,2 до 12Тб.

   Более подробная информация о продукте размещена на официальном веб-сайте изготовителя: https://www.quantum.com/en/products/deduplication-appliances/.

   Функции по хранению, архивированию и восстановлению информации осуществляются посредством программного обеспечения Quantum DX*i* Operating Software версии 3 и версии 4 (где каждая подверсия указанных версий оканчивается на ".nenc", что означает специальную модификацию программного обеспечения, адаптированную для РФ/ЕАЭС), основанного на программной операционной системе CentOS версии 7, являющейся дистрибутивом ядра операционной системы RedHat Enterprise Linux. Указанные специально адаптированные для РФ/ЕАЭС версии программного обеспечения Quantum DX*i* Operating Software относятся исключительно к ограниченному криптографическому функционалу, где часть криптографических функций продукта заблокирована разработчиком, как указано далее.

   Криптографические функции продукта выполняются на уровне программного модуля Software Gui Web Interface (без версии), являющегося компонентом программного обеспечения Quantum DX*i* Operating Software версий 3, 4 (где каждая подверсия указанных версий оканчивается на ".nenc", что означает специальную модификацию программного обеспечения, адаптированную для РФ/ЕАЭС). Криптографические функции реализуются в протоколах публичных криптографических библиотек OpenSSL и OpenSSH (протоколы взаимодействия SSL и SSH) и ограничены функцией аутентификации в виде защиты паролей. Часть криптографических функций заблокирована разработчиком на программном уровне,

такие функции не могут быть в дальнейшем разблокированы, активированы и/или использованы (программный код представлен в бинарном виде, отсутствуют исходный код, протоколы реализации и пользовательский интерфейс).

3. Сведения об изготовителе товара: Квантум Корпорейшн, 224 Эйрпорт Паркуэй, Сьют 300, Сан Хосе, Калифорния 95110, США, номер компании (ID): 94-2665504, тел. +1 408-944-4000, электронная почта: Shawn.Hall@quantum.com, официальный сайт в Интернет: http://www.quantum.com [Quantum Corporation, 224 Airport Parkway, Suite 300, San Jose, California USA 95110. ID: 94-2665504, Shawn Hall, Vice President and General Counsel. tel. +1 408-944-4000, email: Shawn.Hall@quantum.com or Mary.Vigil@Quantum.com].

4. Используемые криптографические алгоритмы (функции) и их назначение: — № категории из приложения № 4

Криптографические функции программного обеспечения Quantum DX*i* Operating Software версий 3, 4 (где каждая подверсия программного обеспечения оканчивается на ".nenc", что означает специальную версию программного обеспечения для РФ), криптографические протоколы SSL, SSH:

а) 3DES, длина ключа 168 бит, используется для защиты ключа дефолтного сертификата в протоколе SSL (защита пароля) — 2.1

б) Ассиметричное шифрование с длиной ключа 128 бит в протоколе SSL реализуется при помощи алгоритмов RSA, Diffie-Hellman, ECDH, SRP и PSK для обмена ключами и проверки их подлинности, а также алгоритмов RSA, DSA и ECDSA для защиты пароля. Данная функция заблокирована изготовителем на программном уровне и не может быть в дальнейшем активирована и/или использована, программный код представлен в бинарном виде, отсутствуют протоколы реализации, исходный код и пользовательский интерфейс — 11

в) Протокол SSH использует хостинговый ключ RSA с длиной ключа 1024 бит или серверный ключ RSA длиной 768 бит для аутентификации в виде защиты пароля. Серверный ключ обновляется каждый час. Продукт обмениваются ключами с клиентом для целей идентификации каждой системы. После подтверждения обмена ключами сессия по передаче данных защищается при помощи алгоритма 3DES с длиной ключа 168 бит, однако функция 3DES заблокирована изготовителем на программном уровне и не может быть в дальнейшем активирована и/или использована, код представлен в бинарном виде, отсутствуют протоколы реализации, исходный код и пользовательский интерфейс — 2.1, 11

г) AES с длиной ключа 256 бит используется для обмена ключами в протоколе SSL. Данная функция заблокирована изготовителем на программном уровне и не может быть в дальнейшем активирована и/или использована, программный код представлен в бинарном виде, отсутствуют протоколы реализации, исходный код и пользовательский интерфейс — 11

д) Стандартный асинхронный интерфейс RS-232 (протоколы SSL, SSH), предназначенный для проверки конфигурации и диагностирования продукта, использует аутентификацию приборов диагностирования в виде защиты пароля, криптографические алгоритмы: хэш-функция SHA-512, MD5 — 2.1

е) Криптографические библиотеки OpenSSL и OpenSSH, используемые в продукте, также по умолчанию содержат стандартные инструкции криптографического преобразования: SHA-AES, HAVAL-TEA, SHA-DES, предназначенные для аутентификации и защиты данных при их передаче. Данные инструкции заблокированы на программном уровне и не могут быть в дальнейшем активированы и/или использованы, код представлен в бинарном виде, отсутствуют протоколы реализации, исходный код и пользовательский интерфейс

11

4. Наличие в товаре функциональных возможностей, не описанных в предоставляемой пользователю эксплуатационной документации: нет.

5. Срок действия нотификации: 31.12.2021.

6. Сведения о заявителе: Александр Андреевич Бычков, гражданин РФ, 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.

7. Сведения о документе изготовителя, удостоверившего полномочия лица на оформление нотификации (при необходимости): Доверенность от 30 ноября 2016 г. (без номера), выданная компанией Квантум Корпорейшн, 224 Эйрпорт Паркуэй, Сьют 300, Сан Хосе, Калифорния 95110, США, 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, код подразделения 770-060, тел +7 (495) 787-27-00.

8. Дата заполнения нотификации: 11.01.2019.

Достоверность и полноту сведений, включенных в нотификацию, подтверждаю:

(Подпись заявителя:) (Александр Андреевич Бычков)
(Ф.И.О.)

RU00000 41066
А.В.ПАРФЕНОВ