40101

Зарегистрировано в реестре " 25 " октября 2018 № RU00000 40101

М.П.

(Подпись лица уполномоченного органа) А.В.ГАРФЕНОВ (Ф.И.О.)

НОТИФИКАЦИЯ
о характеристиках шифровальных (криптографических) средств и товаров, их содержащих

1. Наименование товара: Программно-аппаратный продукт Quantum Xcellis Workflow Director и Xcellis Workflow Extender. А также запасные части к продукту.

   Программное обеспечение: Quantum StorNext File System (SNFS) версия 6, программный интерфейс Telnet command line interface (CLI) без версии.

2. Назначение товара: Программно-аппаратный продукт Quantum Xcellis Workflow Director и Xcellis Workflow Extender - это настраиваемое масштабируемое решение для основного хранилища и высокопроизводительных рабочих процессов с общими данными.

   Для обеспечения бесперебойной работы продукт использует следующие криптографические функции:

   1) Программное обеспечение управления Quantum StorNext File System (SNFS) версия 6, в отношении которой установленным порядком зарегистрирована нотификация № RU0000034230, срок действия до 13.10.2020;

   2) Программный интерфейс Telnet command line interface (CLI) без версии - описание криптографичесих функций указано в пункте 4 настоящей нотификации;

   3) 2 сервера Dell PowerEdge R630 Servers (контроллеры), в отношении которых установленным порядком зарегистрирована нотификация № RU0000021438, срок действия до 31.12.2019.

   Более подробная информация о продукте размещена в открытом доступе на веб-сайте Quantum Corporation в интернет на английском языке по адресу: http://www.quantum.com/products/scale-out-storage/xcellis/index.aspx.

   Интегрированное программное обеспечение Quantum StorNext File System (SNFS) версия 6, в отношении которого установленным порядком зарегистрирована нотификация № RU0000034230, срок действия до 31.12.2019, используется в качестве программного обеспечения управления и использует криптографические функции для целей защиты клиентских настроек от несанкционированного доступа (функции аутентификации). Программный интерфейс Telnet command line interface ((CLI) без версии) позволяет администраторам использовать дополнительные функции аутентификации (авторизации) и обеспечение безопасной работы интерфейсов удаленного управления продуктом в протоколе SSH 2.0 (в публичной криптографической библиотеке OpenSSH), функции веб-сервера через HTTPS с использованием протокола SSL (в публичной криптографической библиотеке OpenSSL), функции интерфейса управления SMI с помощью CIM/XML по протоколу HTTPS опционально с использованием протоколов SSL или SNMPv3 (в публичной криптографической библиотеке OpenSSL). Криптографические функции программного интерфейса Telnet command line interface (CLI) без версии ограничены функциями аутентификации в виде (а) защиты паролей, (б) использования электронной цифровой подписи, и (в) защиты технологических каналов информационно-телекоммуникационных систем и сетей связи (обеспечение удаленного доступа пользователей/администраторов к управлению продуктом/использованию продукта при помощи программного интерфейса, позволяющего запускать, конфигурировать, контролировать и останавливать работу продукта). Продукт не выполняет функции шифрования общих

(пользовательских/клиентских) данных, передаваемых из одного места хранения в другое или в качестве входных или выходных данных на устройство хранения.

3. Сведения об изготовителе товара: Квантум Корпорейшн, 224 Эйрпорт Парквэй, Свит 300, Сан Хосе, Калифорния 95110, США, номер компании (ID): 94-2665504, 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, California USA 95110. ID: 94-2665504, Shawn Hall, Vice President and General Counsel. tel. +1 408-944-4000, email: Mary.Vigil@Quantum.com, official website: http://www.quantum.com].

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

4.1. Криптографические функции программного обеспечения Quantum StorNext File System (SNFS) версия 6:

а) криптографические функции указаны в зарегистрированной установленным порядком нотификации № RU0000034230, срок действия до 13.10.2020 — 2(1); 2(2)

4.2. Криптографические функции программного интерфейса Telnet command line interface (CLI) без версии:

а) Криптографические алгоритмы имплементации протокола SSL (с использованием публичной криптографической библиотеки OpenSSL): RSA, асимметричный, максимальная длина ключа 2048 бит, вместе с симметричным алгоритмом Camelia 256 CBC-SHA, максимальная длина ключа 256 бит, выполняемые функции: авторизация доступа администратора (аутентификация в виде защиты паролей и использования электронной цифровой подписи), защита канала удаленного управления (данные о запуске продукта, его конфигурации, мониторинге и остановке) — 2(1); 2(2); 10

б) Криптографические алгоритмы имплементации протокола SSH 2.0: AES-CBC, симметричный, максимальная длина ключа 128 and 192 бит; Arcfour, симметричный максимальная длина ключа 128 и 256 бит; Rinjdael, симметричный максимальная длина ключа 128, 192, 256 бит; RSA, асимметричный, максимальная длина ключа 2048 бит; DSA, асимметричный, максимальная длина ключа 1024 бит; выполняемые функции: авторизация доступа администратора (аутентификация в виде защиты паролей и использования электронной цифровой подписи), защита канала удаленного управления (данные о запуске продукта, его конфигурации, мониторинге и остановке) — 2(1); 2(2); 10

в) Криптографические алгоритмы имплементации протокола SNMPv3 (поддерживаемые в публичной криптографической библиотеке OpenSSL): MD5 (HMAC-MD5-96), хэш-функция, максимальная длина ключа 96 бит, SHA (HMAC-SHA-96), хэш-функция, максимальная длина ключа 96 бит; DES (CBC-DES-56), симметричный, максимальная длина ключа 56 бит; AES, симметричный, максимальная длина ключа 128 бит; выполняемые функции: авторизация доступа администратора (аутентификация в виде защиты — 2(1), 2(2), 10

паролей и использования электронной цифровой подписи), защита канала удаленного управления (данные о запуске продукта, его конфигурации, мониторинге и остановке)

г) Криптографические алгоритмы имплементации протокола SMI-S (CIM/XML), с использованием протоколов SSL или SNMPv3 через соединение https (с использованием публичной криптографической библиотеки OpenSSL): SHA1 (хэш-функция) вместе с RSA (асимметричный алгоритм), максимальная длина ключа 2048 бит; выполняемые функции: авторизация доступа администратора (аутентификация в виде защиты паролей и использования электронной цифровой подписи)

2(1), 2(2)

4.3. Криптографические функции серверов Dell PowerEdge R630 Servers (контроллеров):

а) криптографические функции указаны в зарегистрированной установленным порядком нотификации № RU0000021438, срок действия до 31.12.2019

2, 3, 6

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

6. Срок действия нотификации: 31.12.2019.

7. 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.

8. Сведения о документе изготовителя, удостоверившего полномочия лица на оформление нотификации (при необходимости): Доверенность от 30 ноября 2016 г. (без номера), выданная компанией Квантум Корпорейшн, 227 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.

9. Дата заполнения нотификации: 23.10.2018.

Достоверность и полноту сведений, включенных в нотификацию, подтверждаю:

(Подпись заявителя)

(Александр Андреевич Бычков)

(Ф.И.О.)

Центр по лицензированию, сертификации и защите государственной тайны Федеральной службы безопасности Российской Федерации

RU00000 40101

А.В.ПАРФЕНОВ