SIEMENS

Департамент
«Управление электроэнергией»

Организациям электроэнергетики

Компания ООО «Сименс»
Департамент EM DG
Фамилия Горенков С.Д.
Факс +7 (495) 737-23-85

E-mail Sergey.Gorenkov@siemens.com

Вх. №
Исх. № EM DG – 104
Дата 19.04.2018

Информационное письмо

Настоящим информационным письмом уведомляем конечных пользователей продукции компании SIEMENS о разработанных к применению технических решениях и рекомендациях компании SIEMENS по обеспечению информационной безопасности и устранению выявленных уязвимостей в сериях устройств SIPROTEC 4, SIPROTEC Compact, Reyrolle и сервисном ПО DIGSI 4

Уязвимость CVE-2018-4838:
Краткое описание: WEB интерфейс МП устройства позволял неавторизованному пользователю обновить встроенное программное обеспечение коммуникационного модуля EN100, в том числе применить более ранние версии с известными уязвимостями

Уязвимость CVE-2018-4839:
Краткое описание: Злоумышленник при наличии локального доступа к сервисному инструменту DIGSI 4 или прямого доступа в локальную сеть объекта и возможности считывания определенного сетевого трафика в этой сети имел возможность восстановить пароли доступа к МП устройству

Уязвимость CVE-2018-4840:
Краткое описание: Механизмы сервисного обслуживания DIGSI 4 позволяли неавторизованному стороннему пользователю загружать измененную конфигурацию в МП устройство с новыми паролями доступа

Необходимо отдельно отметить тот факт, что приведенные выше уязвимости могут иметь негативное влияние на информационную безопасность объекта в том случае, когда у злоумышленника, хорошо знающего МП защиты SIPROTEC и программное обеспечение DIGSI 4, имеется физический или удаленный доступ к критически важной информационной сети Ethernet объекта.

Как главную и основную меру обеспечения информационной безопасности SIEMENS настоятельно рекомендует обеспечивать информационную защиту всей локальной сети объекта от умышленных атак извне соответствующими внешними сетевыми механизмами, например: Firewall, сегментация, VPN, а также соответствующими организационными мероприятиями и регламентами. Информационная сеть объекта с критически важными процессами и МП устройствами разных производителей должна иметь надежную защиту от внешних атак.

В целях устранения выявленных уязвимостей в продукции SIEMENS описанных выше, по решению конечного пользователя в рамках планового технического обслуживания рекомендуются следующие обновления встроенного программного обеспечения МП устройств и сервисного ПО:

Продукт	Версия	Рекомендация
Ethernet модуль **EN100** с протоколом МЭК 61850	Все версии < 4.30	Обновить встроенное ПО модулей EN100-E+ и EN100-O+ до версии 4.30 и настроить сервисный пароль Для остальных модулей EN100 рекомендации будут выпущены отдельным информационным письмом
DIGSI 4	Все версии < 4.92	Обновить сервисное ПО DIGSI 4 до версии 4.92
SIPROTEC Compact **7SJ80**	Все версии < 4.77	Обновить встроенное ПО 7SJ80 до версии 4.77
SIPROTEC Compact **7SK80**	Все версии < 4.77	Обновить встроенное ПО 7SK80 до версии 4.77
SIPROTEC 4 **7SJ66**	Все версии < 4.30	Обновить встроенное ПО 7SJ66 до версии 4.30

С уважением,

С.Д. Горенков

Руководитель технического центра
EM DG, ООО «Сименс»