НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200727.2 | 27 июля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Schneider Electric Tricon Communication Module

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты Программно-аппаратное решение
Уязвимое ПО	Triconex TriStation 1131: -, 4.12.0 Tricon Communications Module (TCM) Models 4351: -, 10.5.3 Tricon Communications Module (TCM) Models 4352: -, 10.5.3 Tricon Communications Module (TCM) Models 4351A/B: -, 10.5.3 Tricon Communications Module (TCM) Models 4352A/B: -, 10.5.3
Дата выявления	14 апреля 2020 г.
Дата обновления	23 июня 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-7484 CVE-2020-7486	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного вредоносного сетевого пакета. Уязвимость обусловлена некорректным управлением внутренними ресурсами. CVSS:3.0 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов)	7.5

	Рекомендации по устранению: обновить программное обеспечение.	
MITRE: CVE-2020-7491	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректным разграничением доступа к устаревшей учетной записи отладочного порта. CVSS:3.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: обновить программное обеспечение.	10.0

Ссылки на источники	https://www.se.com/ww/en/download/document/SESB-2020-105-01/