

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210611.6 | 11 июня 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Отказ в обслуживании в Siemens SIMATIC RFID Readers

Идентификатор уязвимости	MITRE: CVE-2021-31340
Идентификатор программной ошибки	CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным использованием внутренних ресурсов уязвимой службой.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	SIMATIC RF166C: v1.1 SIMATIC RF185C: v1.1 SIMATIC RF186C: v1.1 SIMATIC RF186CI: v1.1 SIMATIC RF188C: v1.1 SIMATIC RF188CI: v1.1 SIMATIC RF360R: все версии SIMATIC RF615R: до v3.0 SIMATIC RF680R: до v3.0 SIMATIC RF685R: до v3.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	10 июня 2021 г.
Дата обновления	10 июня 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)

Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	<a href="https://www.cybersecurity-help.cz/vdb/SB2021061004">https://www.cybersecurity-help.cz/vdb/SB2021061004</a> <a href="https://cert-portal.siemens.com/productcert/pdf/ssa-787292.pdf">https://cert-portal.siemens.com/productcert/pdf/ssa-787292.pdf</a> <a href="https://us-cert.cisa.gov/ics/advisories/icsa-21-159-13">https://us-cert.cisa.gov/ics/advisories/icsa-21-159-13</a>