

# 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-20200611.8 | 11 июня 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Переполнение буфера в WebAccess Node

Идентификатор уязвимости	MITRE: CVE-2020-12019
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код на целевом устройстве. Уязвимость обусловлена некорректным определением границ буфера памяти.
Категория уязвимого продукта	IoT-устройства
Уязвимое ПО	WebAccess Scada Node: 8.4.4
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 июня 2020 г.
Дата обновления	10 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/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)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств	Наличие не подтверждено

эксплуатации

Наличие средств устранения  
уязвимости

Официальное решение

Достоверность сведений об  
уязвимости

Сведения подтверждены

---

Ссылки на источники

<https://www.cybersecurity-help.cz/vdb/SB2020061028>