

# 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 УЯЗВИМОСТЯХ

VULN-20201013.2 | 13 октября 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Множественные уязвимости в контроллерах WAGO

Категория уязвимого продукта	Промышленное программно-аппаратное оборудование
Уязвимый продукт	WAGO 750-8XX до vFW07 WAGO 750-36X и WAGO 750-8XX до vFW03c
Дата выявления	30 сентябрь 2020 г.
Дата обновления	30 сентябрь 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-12505	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:U/RL:O/RC:C CWE-287: Некорректная аутентификация</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p>	8.2

MITRE:  
CVE-2020-12506

Эксплуатация уязвимости позволяет удаленному злоумышленнику изменить настройки на целевом устройстве посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в веб-интерфейсе управления.

CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C  
CWE-287: Некорректная аутентификация

Рекомендации по устранению: обновить программное обеспечение.

9.1

Ссылки на  
источники

<https://cert.vde.com/de-de/advisories/vde-2020-027>

<https://cert.vde.com/de-de/advisories/vde-2020-028>