

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220426.1 | 26 апреля 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Множественные уязвимости в FortiWAN

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	FortiWAN: до 4.5.9
Дата выявления	06 апреля 2022 г.
Дата обновления	06 апреля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-26112	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольный код в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-787: Запись за границами буфера</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	9.8

<p>MITRE: CVE-2021-24009</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольные команды в целевой системе посредством отправки специально сформированных HTTP-запросов. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>8.8</p>
<p>MITRE: CVE-2021-34798</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнять произвольные команды в целевой системе посредством отправки специально сформированных HTTP-запросов. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</p> <p>CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>	<p>9.8</p>

Ссылки на  
источники

<https://www.fortiguard.com/psirt/FG-IR-21-060>  
<https://www.fortiguard.com/psirt/FG-IR-21-065>