

# 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-20210112.4 | 12 января 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Fortinet FortiWeb

Идентификатор уязвимости	MITRE: CVE-2020-29016
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной обработкой длины имени сертификата.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	Fortinet FortiWeb: 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 января 2021 г.
Дата обновления	5 января 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкий (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 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/SB2021010513">https://www.cybersecurity-help.cz/vdb/SB2021010513</a>