

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](https://cert.gov.ru)

E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211021.6 | 21 октября 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в strongSwan

Идентификатор уязвимости	MITRE: CVE-2021-41991 CVE-2021-41990
Идентификатор программной ошибки	CWE-190: Целочисленное переполнение или циклический возврат
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением при обработке сертификатов.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	strongSwan: 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.1.0, 5.1.1, 5.1.2, 5.1.3, 5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.4.0, 5.5.0, 5.5.1, 5.5.2, 5.5.3, 5.6.0, 5.6.1, 5.6.2, 5.6.3, 5.7.0, 5.7.1, 5.7.2, 5.8.0, 5.8.1, 5.8.2, 5.8.3, 5.8.4, 5.9.0, 5.9.1, 5.9.2, 5.9.3
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 октября 2021 г.
Дата обновления	19 октября 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)	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 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/SB2021101946">https://www.cybersecurity-help.cz/vdb/SB2021101946</a> <a href="http://www.strongswan.org/blog/2021/10/18/strongswan-vulnerability-(cve-2021-41991).html">http://www.strongswan.org/blog/2021/10/18/strongswan-vulnerability-(cve-2021-41991).html</a> <a href="http://github.com/strongswan/strongswan/releases/tag/5.9.4">http://github.com/strongswan/strongswan/releases/tag/5.9.4</a>