

# 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-20210915.4 | 15 сентября 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Siemens NX

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	NX 1980: before 1984
Дата выявления	15 сентября 2021 г.
Дата обновления	15 сентября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-37202	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой использования после освобождения.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-416: Использование после освобождения</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.8
MITRE: CVE-2021-37203	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена</p>	8.1

CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C

CWE-125: Чтение за пределами буфера

Рекомендации по устранению: обновить программное обеспечение

Ссылки на  
источники

<https://www.cybersecurity-help.cz/vdb/SB2021091517>

<https://cert-portal.siemens.com/productcert/pdf/ssa-208530.pdf>