

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220222.5 | 22 февраля 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Siemens Simcenter Femap

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Simcenter Femap: до 2022.1.1
Дата выявления	17 февраля 2022 г.
Дата обновления	17 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-46162	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного NEU-файла. Уязвимость обусловлена ошибкой границ памяти.</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-787: Запись за границами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.8

MITRE: CVE-2021-46699	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного BDF-файла. Уязвимость обусловлена ошибкой границ памяти.</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-121: Переполнение буфера в стеке</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.8
Ссылки на источники	<p>http://cert-portal.siemens.com/productcert/txt/ssa-949188.txt</p> <p>https://www.cybersecurity-help.cz/vdb/SB2022021725</p>	