НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221213.5 | 13 декабря 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в cflinuxfs3

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	cflinuxfs3: 0.0.0 - 0.343.0
Дата выявления	6 декабря 2022 г.
Дата обновления	6 декабря 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-40303	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H CWE-190: Целочисленное переполнение или циклический возврат 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.	7.5

MITRE: CVE-2022-40304	Эксплуатация уязвимости позволяет локальному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена некорректной обработкой ссылочных циклов. CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-399: Уязвимости, связанные с управлением ресурсами 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.	7.8

Ссылки на источники	http://github.com/cloudfoundry/cflinuxfs3/releases/tag/0.344.0 https://bdu.fstec.ru/vul/2022-06700 https://bdu.fstec.ru/vul/2022-06701