НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211224.13 | 24 декабря 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в CF Deployment

Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	CF Deployment: 17.0.0
Дата выявления	21 декабря 2021 г.
Дата обновления	21 декабря 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-44228	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-94: Некорректное управление генерированием кода (внедрение кода) Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2021-45046	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных вредоносных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-94: Некорректное управление генерированием кода (внедрение кода) Рекомендации по устранению: обновить программное обеспечение	9.0

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021122018 http://github.com/cloudfoundry/cf-deployment/releases/tag/v17.1.0