НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230213.1 | 13 февраля 2023 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Red Hat OpenShift Container Platform

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Red Hat OpenShift Container Platform: 4.9.0 - 4.9.54
Дата выявления	13 февраля 2023 г.
Дата обновления	13 февраля 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-4238	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к конфиденциальной информации. Уязвимость обусловлена недостаточной энтропией при генерации буквенно-цифровых строк в функциях RandomAlphaNumeric и CryptoRandomAlphaNumeric. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H CWE-331: Недостаточная энтропия 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.	9.1

MITRE: CVE-2022-41912	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной обработкой ответов SAML. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N CWE-287: Некорректная аутентификация 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.	9.1

Ссылки на источники	http://access.redhat.com/errata/RHSA-2023:0574