НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220209.3 | 9 февраля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Red Hat Virtualization

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	redhat-virtualization-host (Red Hat package): до 4.3.20-20211202.1.el7_9 redhat-release-virtualization-host (Red Hat package): до 4.3.20-1.el7ev Red Hat Virtualization Host: 4 Red Hat Virtualization: 4
Дата выявления	8 февраля 2022 г.
Дата обновления	8 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-25717	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение	8.1

MITRE: CVE-2021-4034	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнять произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:U/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	8.8

Ссылки на источники	http://access.redhat.com/errata/RHSA-2022:0443 https://www.cybersecurity-help.cz/vdb/SB2022020813