НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220211.4 | 11 февраля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Red Hat Virtualization Manager

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	ovirt-engine (Red Hat package): 4.4.4.5-0.10.el8ev, 4.4.7.6-0.11.el8ev, 4.4.9.2-0.6.el8ev rhvm-branding-rhv (Red Hat package): 4.4.7-1.el8ev, 4.4.9-1.el8ev Red Hat Virtualization Manager: 4.4 snmp4j (Red Hat package): до 3.6.4-0.1.el8ev
Дата выявления	9 февраля 2022 г.
Дата обновления	9 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-4104	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-502: Десериализация недоверенных данных Рекомендации по устранению: обновить программное обеспечение	8.1

MITRE: CVE-2022-23302 CVE-2022-23307 CVE-2020-9493	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-502: Десериализация недоверенных данных Рекомендации по устранению: обновить программное обеспечение	9.8

Ссылки на источники	http://access.redhat.com/errata/RHSA-2022:0475 https://www.cybersecurity-help.cz/vdb/SB2022020933