НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220408.7 | 8 апреля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в VMware vRealize Automation

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	vRealize Automation: 7.6
Дата выявления	06 апреля 2022 г.
Дата обновления	06 апреля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-22959	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды ОС в целевой системе отправки специального сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-352: Подделка межсайтового запроса (CSRF) 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.	9.3

MITRE: CVE-2022-22960	Эксплуатация уязвимости позволяет удаленному злоумышленнику атаки типа CSRF посредством открытия пользователем специального созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой источника HTTP-запроса. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N/E:U/RL:O/RC:C] CWE-276: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) 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.	9.3

Ссылки на источники	http://www.vmware.com/security/advisories/VMSA-2022-0011.html http://kb.vmware.com/s/article/88099