НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220405.3 | 5 апреля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Rizin

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Rizin: 0.1.0 - 0.3.1
Дата выявления	05 апреля 2022 г.
Дата обновления	05 апреля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-43814	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специального созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-787: Запись за границами буфера 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.	8.8

MITRE: CVE-2021-4022	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специального созданного вредоносного файла. Уязвимость обусловлена ошибкой использования после освобождения. CVSSv3.0: AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения 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.	8.8

Ссылки на источники	http://github.com/rizinorg/rizin/issues/2083 http://github.com/rizinorg/rizin/security/advisories/GHSA-hqqp-vjcm-mw8r http://github.com/rizinorg/rizin/commit/aa6917772d2f32e5a7daab25a46c72df0b5ea406 http://github.com/rizinorg/rizin/issues/2015 http://github.com/rizinorg/rizin/pull/2031 http://github.com/rizinorg/rizin/commit/21584e416cdcef2fa7d855c5aabf592a965f0e8d http://github.com/rizinorg/rizin/commit/6ce71d8aa3dafe3cdb52d5d72ae8f4b95916f939