НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220914.34 | 14 сентября 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Rizin

Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	Rizin: 0.1.0 - 0.4.0
Дата выявления	12 сентября 2022 г.
Дата обновления	12 сентября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-36039 CVE-2022-36040 CVE-2022-36041 CVE-2022-36042 CVE-2022-36044	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально 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-2022-36043	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена граничной ошибкой в функции. 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-415: Двойное освобождение 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/commit/07b43bc8aa1ffebd9b68d60624c9610cf7e460c7 http://github.com/rizinorg/rizin/issues/2969 http://github.com/rizinorg/rizin/security/advisories/GHSA-h897-rhm9-rpmw http://github.com/rizinorg/rizin/commit/1524f85211445e41506f98180f8f69f7bf115406 http://github.com/rizinorg/rizin/commit/05bbd147caccc60162d6fba9baaaf24befa281cd http://github.com/rizinorg/rizin/issues/2964 http://github.com/rizinorg/rizin/issues/2963 http://github.com/rizinorg/rizin/security/advisories/GHSA-pr85-hv85-45pg http://github.com/rizinorg/rizin/commit/a3d50c1ea185f3f642f2d8180715f82d98840784 http://github.com/rizinorg/rizin/security/advisories/GHSA-rjhv-mj4g-j4p5 http://github.com/rizinorg/rizin/security/advisories/GHSA-2c7m-2f37-mr5m http://github.com/rizinorg/rizin/commit/556ca2f9eef01ec0f4a76d1fbacfcf3a87a44810 http://github.com/rizinorg/rizin/commit/7323e64d68ecccfb0ed3ee480f704384c38676b2 http://github.com/rizinorg/rizin/commit/68948017423a12786704e54227b8b2f918c2fd27 http://github.com/rizinorg/rizin/security/advisories/GHSA-pf72-jg54-8gvp http://github.com/rizinorg/rizin/issues/2956 http://github.com/rizinorg/rizin/security/advisories/GHSA-mqcj-82c6-gh5q