# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220914.35 | 14 сентября 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## НСД в KubeVela

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2022-36089 |
| Идентификатор программной ошибки | CWE-294: Обход аутентификации при помощи перехвата и воспроизведения |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена раскрытием идентификатора платформы. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | KubeVela: 1.4.0 - 1.5.2 |
| 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. |
| Дата выявления | 9 сентября 2022 г. |
| Дата обновления | 9 сентября 2022 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Отсутствует (N) |
| Необходимость взаимодействия с пользователем (UI) | Отсутствует (N) |
| Масштаб последствий эксплуатации | Не изменяется (U) |

| | |
|---|---|
| уязвимости (S) | |
| Влияние на конфиденциальность (C) | Низкое (L) |
| Влияние на целостность (I) | Высокое (H) |
| Влияние на доступность (A) | Отсутствует (N) |
| Степень зрелости доступных средств эксплуатации | Наличие не подтверждено |
| Наличие средств устранения уязвимости | Официальное решение |
| Достоверность сведений об уязвимости | Сведения подтверждены |
| Ссылки на источники | http://github.com/kubevela/kubevela/pull/4634<br>http://github.com/kubevela/kubevela/security/advisories/GHSA-cq42-w295-r29q |