

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220327.2 | 27 марта 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Повышение привилегий в Argo CD

Идентификатор уязвимости	MITRE: CVE-2022-24768 CVE-2022-1025
Идентификатор программной ошибки	CWE-284: Некорректное управление доступом
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректным ограничением доступа.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Argo CD: 2.1.0 - 2.1.13, 2.3.0 - 2.3.1, 2.2.0 - 2.2.7, 2.0.0 - 2.0.5, 1.7.0 - 1.7.14, 1.8.0 - 1.8.7, 1.6.0 - 1.6.2, 1.5.0 - 1.5.8, 1.4.0 - 1.4.3, 1.3.0 - 1.3.6, 1.2.0 - 1.2.5, 1.1.0 - 1.1.2, 1.0.0 - 1.0.2, 0.7.0 - 0.7.2, 0.6.0 - 0.6.2, 0.5.0 - 0.5.4
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	24 марта 2022 г.
Дата обновления	24 марта 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с	Низкий (L)

пользователем (UI)

Масштаб последствий эксплуатации уязвимости (S)

Изменяется (C)

Влияние на конфиденциальность (C)

Высокое (H)

Влияние на целостность (I)

Высокое (H)

Влияние на доступность (A)

Высокое (H)

Степень зрелости доступных средств эксплуатации

Наличие не подтверждено

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Сведения подтверждены

---

Ссылки на источники

<https://www.cybersecurity-help.cz/vdb/SB2022032406>

<http://github.com/argoproj/argo->

<cd/security/advisories/GHSA-2f5v-8r3f-8pww>