НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220524.13 | 24 мая 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

НСД в Argo CD

Идентификатор уязвимости	MITRE: CVE-2022-29165
Идентификатор программной ошибки	CWE-290: Обход аутентификации, связанный с подменой данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально созданного веб-токена JSON (JWT) вместе с запросом. Уязвимость обусловлена ошибкой в процессе проверки подлинности.
Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимый продукт	Argo CD: 2.3.0 - 2.3.3, 2.2.0 - 2.2.8, 2.1.0 - 2.1.14, 2.0.0 - 2.0.5, 1.8.0 - 1.8.7, 1.7.0 - 1.7.14, 1.6.0 - 1.6.2, 1.5.0 - 1.5.8, 1.4.0 - 1.4.3
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	19 мая 2022 г.
Дата обновления	19 мая 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C
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 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	http://bugzilla.redhat.com/show_bug.cgi?id=2081686 http://github.com/argoproj/argo-cd/security/advisories/GHSA-r642-gv9p-2wjj