НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220526.9 | 26 мая 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

НСД в countly-server

Идентификатор уязвимости	MITRE: CVE-2022-29174
Идентификатор программной ошибки	CWE-254: Уязвимости в безопасности ПО
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена предсказуемым маркером сброс пароля.
Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимый продукт	countly-server: 21.11 - 22.03.6.2
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	24 мая 2022 г.
Дата обновления	24 мая 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.1 AV:N/AC:H/PR:N/UI:N/S:U/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)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)

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://github.com/Countly/countly-server/commit/2bfa1ee1fa46e9bb007cf8687ad197ab9c604999 http://github.com/Countly/countly-server/security/advisories/GHSA-98vh-wqw5-p23v