НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201030.10 | 30 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в CMS Strapi

Идентификатор уязвимости	MITRE: CVE-2020-27665
Идентификатор программной ошибки	CWE-276: Некорректные разрешения, назначаемые по умолчанию
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить привилегии в целевой системе путем отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным функционированием механизма управления доступом.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Strapi: 3.2.0, 3.2.1, 3.2.2, 3.2.3, 3.2.4
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 октября 2020 г.
Дата обновления	27 октября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/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 уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)

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	https://github.com/strapi/strapi/releases/tag/v3.2.5 https://nvd.nist.gov/vuln/detail/CVE-2020-27665