

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220621.11 | 21 июня 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Spring Data MongoDB

Идентификатор уязвимости	MITRE: CVE-2022-22980
Идентификатор программной ошибки	CWE-917: Некорректная нейтрализация специальных элементов, используемых в утверждениях языка выражений (внедрение кода языка выражений)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных SpEL-запросов. Уязвимость обусловлена некорректной проверкой ввода.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Spring Data MongoDB: 3.3.0 - 3.4.0
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	21 июня 2022 г.
Дата обновления	21 июня 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.0 AV:N/AC:H/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)	Высокая (H)
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

<https://tanzu.vmware.com/security/cve-2022-22980>