НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200727.1 | 27 июля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в Spring Integration

Идентификатор уязвимости	MITRE: CVE-2020-5413
Идентификатор программной ошибки	CWE-502: Десериализация недоверенных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного сетевого пакета. Уязвимость обусловлена десериализацией недоверенных данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Spring Integration до v4.3.23, v5.1.12, v5.2.8, v5.3.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 июля 2020 г.
Дата обновления	24 июля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/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 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	https://spring.io/blog/2020/07/22/spring-integration-4-3-23-5-1-12-5-2-8-5-3-2-available-cve-2020-5413 https://tanzu.vmware.com/security/cve-2020-5413 https://www.cybersecurity-help.cz/vdb/SB2020072408