НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200603.3| 3 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Несанкционированный доступ к данным в Pivotal Spring Cloud Config

Идентификатор уязвимости	MITRE: CVE-2020-5410
Идентификатор программной ошибки	CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной проверкой предоставленных пользователем данных в модуле spring-cloud-config-server.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Spring Cloud Config до v2.2.3, v2.1.9
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	1 июня 2020 г.
Дата обновления	1 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкий (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)	Отсутствует (N)
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://tanzu.vmware.com/security/cve-2020-5410 https://www.cybersecurity-help.cz/vdb/SB2020060202