НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211224.10 | 24 декабря 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в ModSecurity

Идентификатор уязвимости	MITRE: CVE-2021-42717
Идентификатор программной ошибки	CWE-674: Неконтролируемая рекурсия
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена неконтролируемой рекурсией при обработке JSON-объектов.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	ModSecurity: до 3.0.5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 декабря 2021 г.
Дата обновления	19 декабря 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)

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://www.cybersecurity-help.cz/vdb/SB2021121901 http://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/modsecurity-dos-vulnerability-in-json-parsing-cve-2021-42717/