НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211130.9 | 30 ноября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Чтение произвольных файлов в Apache APISIX

Идентификатор уязвимости	MITRE: CVE-2021-43557
Идентификатор программной ошибки	CWE-22: Некорректные ограничения путей для каталогов (выход за пределы каталога)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать произвольный файлы в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке последовательностей обхода каталогов.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Apache APISIX: 2.10.0, 2.10.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	26 ноября 2021 г.
Дата обновления	26 ноября 2021 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)	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)	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://www.cybersecurity-help.cz/vdb/SB2021112611 http://lists.apache.org/thread/18jyd458ptocr31rnkjs71w4h366mv7h http://www.openwall.com/lists/oss-security/2021/11/22/2 http://www.openwall.com/lists/oss-security/2021/11/22/1 http://www.openwall.com/lists/oss-security/2021/11/23/1