НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211126.3 | 26 ноября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Juniper Networks Junos OS

Идентификатор уязвимости	MITRE: CVE-2021-31383
Идентификатор программной ошибки	CWE-787: Запись за границами буфера CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Juniper Networks версий Junos OS 19.2 до 19.2R3-S2; Версии 19.3 до 19.3R2-S6, 19.3R3-S2; Версии 19.4 до 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; Версии 20.1 до 20.1R2-S2, 20.1R3; Версии 20.2 до 20.2R2-S3, 20.2R3; 20.3 до 20.3R2.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 октября 2021 г.
Дата обновления	19 октября 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://nvd.nist.gov/vuln/detail/CVE-2021-31383 https://kb.juniper.net/JSA11251