

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ
VULN-20201127.4 | 27 ноября 2020 г.
Уровень опасности: **ВЫСОКИЙ**
Наличие обновления: **ЕСТЬ**

Отказ в обслуживании в Juniper OS Junos

Идентификатор уязвимости	MITRE: CVE-2020-1684
Идентификатор программной ошибки	CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных HTTP-пакетов при включенной проверке идентификаторов приложений. Уязвимость обусловлена некорректной обработкой HTTP-пакетов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Juniper Junos OS: 12.3X48, 15.1X49, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4. Для платформ серии SRX.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 октября 2020 г.
Дата обновления	28 октября 2020 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://kb.juniper.net/JSA11081>

<https://nvd.nist.gov/vuln/detail/CVE-2020-1684>