НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210210.13 | 10 февраля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Junos OS

Идентификатор уязвимости	MITRE: CVE-2021-0217
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных DHCP-пакетов. Уязвимость обусловлена некорректной обработкой входящих DHCP-пакетов, вызывающих исчерпание выделенной DMA памяти.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Junos OS 17.4R3, 18.1R3, 18.2R3, 18.3R3, 18.4R2, 18.4R3, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 января 2021 г.
Дата обновления	28 января 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.4 AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
Вектор атаки (AV)	Смежная сеть (A)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
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/JSA11107 https://nvd.nist.gov/vuln/detail/CVE-2021-0217