

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220114.17 | 14 января 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Отказ в обслуживании в Juniper Junos OS IPv6

Идентификатор уязвимости	MITRE: CVE-2022-22174
Идентификатор программной ошибки	CWE-401: Некорректное освобождение памяти до удаления последней ссылки (утечка памяти)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной обработкой входящих пакетов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Juniper Junos OS: до 21.4R1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	12 января 2022 г.
Дата обновления	12 января 2022 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/SB2022011227>
http://kb.juniper.net/InfoCenter/index?page=content&id=JS-A11280&cat=SIRT_1&actp=LIST