

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210406.2 | 6 апреля 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в ОС Junos и ОС Junos Evolved

Идентификатор уязвимости	MITRE: CVE-2021-0208
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании или выполнить произвольный код в целевой системе посредством отправки специально созданных RSVP-пакетов. Уязвимость обусловлена некорректной проверкой входных данных в Routing Protocol Daemon (RPD).
Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	Juniper Junos OS: до 15.1X49-D240, 17.3R3-S10, 17.4R3-S2, 18.1R3-S10, 18.2R2-S7, 18.2R3-S4, 18.3R3-S2, 18.4R1-S8, 18.4R2-S6, 18.4R3-S2, 19.1R1-S5, 19.1R3-S3, 19.2R3, 19.3R2-S5, 19.3R3, 19.4R2-S2, 19.4R3-S1, 20.1R1-S4, 20.1R2, 20.2R1 Junos OS Evolved: до 19.3R2-S5-EVO, 19.4R2-S2-EVO, 20.1R1-S4-EVO
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 января 2021 г.
Дата обновления	15 января 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Смежная сеть (A)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с	Отсутствует (N)

пользователем (UI)

Масштаб последствий эксплуатации уязвимости (S)

Не изменяется (U)

Влияние на конфиденциальность (C)

Высокое (H)

Влияние на целостность (I)

Высокое (H)

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/SB2021011548>
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11098&cat=SIRT_1&actp=LIST