# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210210.8 | 10 февраля 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

## Отказ в обслуживании в Junos OS и Junos OS Evolved

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2021-0211 |
| Идентификатор программной ошибки | CWE-754: Некорректная проверка наличия нестандартных условий или исключений |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных сетевых пакетов по протоколу BGP FlowSpec. Уязвимость обусловлена некорректной обработкой входных данных в службе Routing Protocol Daemon (RPD). |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимый продукт | OS Junos v15.1, 15.1X49, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3.<br>Junos OS Evolved v20.3 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 15 января 2021 г. |
| Дата обновления | 22 января 2021 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/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) | Изменяется (C) |

| | |
|---|---|
| Влияние на конфиденциальность (C) | Отсутствует (N) |
| 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://kb.juniper.net/JSA11101<br>https://nvd.nist.gov/vuln/detail/CVE-2021-0211 |