

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191206.2 | 6 декабря 2019 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Уязвимость реализации протокола OSPF в Junos OS

Идентификатор уязвимости	MITRE: CVE-2019-0056 JUNIPER: JSA10954 BDU: 2019-03655
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных CWE-410: Недостаточный пул ресурсов
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному неаутентифицированному злоумышленнику вызвать отказ в обслуживании в целевой системе путем отправки большого количества легитимных IPv6-пакетов определенных типов. Уязвимость обусловлена недостаточностью пула ресурсов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Junos OS для MX480, MX960, MX2008, MX2010, MX2020: от v18.1 до v18.1R2-S4, v18.1R3-S5; от v18.1X75 до v18.1X75-D10 и более поздние версии; от v18.2 до v18.2R1-S5, v18.2R2-S3, v18.2R3; от v18.2X75 до v18.2X75-D50; от v18.3 до v18.3R1-S4, v18.3R2, v18.3R3; от v18.4 до v18.4R1-S2, v18.4R2.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 октября 2019 г.
Дата обновления	17 октября 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
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 (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)

---

Ссылки на источники

<https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10954&actp=METADATA>  
<https://nvd.nist.gov/vuln/detail/CVE-2019-0056>