НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191021.1 | 21 октября 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость процесса srxpfe Junos OS

Идентификатор уязвимости	MITRE: CVE-2019-0075 Juniper: JSA10976 BDU: 2019-03806
Идентификатор программной ошибки	CWE-400: Неконтролируемое потребление ресурсов
Описание уязвимости	Эксплуатация уязвимости в процессе srxpfe Junos OS позволяет злоумышленнику вызвать отказ в обслуживании оборудования посредством отправки большого количества сетевых пакетов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Junos OS версий 12.3X48-12.3X48-D80, 15.1X49-15.1X49-D160, 17.3-17.3R3-S7 17.4-17.4R2-S8, 17.4R3, 18.1-18.1R3-S8, 18.2-18.2R2, 18.3-18.3R2.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 октября 2019 г.
Дата обновления	21 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)	Не требуется (N)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутсвует (N)

Влияние на целостность (I)	Отсутсвует (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/JSA10976