НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201125.3| 25 ноября 2020

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Juniper ОС Junos

Идентификатор уязвимости	MITRE: CVE-2020-1679
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного сетевого пакета. Уязвимость обусловлена некорректной обработкой сетевых пакетов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	ОС Junos: 17.2X75, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1 Затронутые платформы: PTX, QFX.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	14 октября 2020 г.
Дата обновления	28 октября2020 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://kb.juniper.net/InfoCenter/index?page=content&id=JSA11076&actp=METADATA