НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200610.4| 10 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в маршрутизаторах Juniper PTX1000, PTX10000 и QFX10000.

Идентификатор уязвимости	MITRE: CVE-2020-1617
Идентификатор программной ошибки	CWE-665: Некорректная инициализация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально сформированных вредоносных сетевых пакетов. Уязвимость обусловлена некорректным управлением памятью при проверке сетевых пакетов в sFlow.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	ОС Junos 17.4, 18.1, 18.2, 18.2X75, 18.3.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 апреля 2020 г.
Дата обновления	21 апреля 2020 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/JSA11000