

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200615.1 | 15 июня 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Отказ в обслуживании в Juniper Networks Junos OS и Junos OS Evolved

Идентификатор уязвимости	MITRE: CVE-2020-1638
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 сформированных вредоносных сетевых пакетов. Уязвимость обусловлена некорректной работой компонента Flexible PIC Concentrators.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	ОС Junos до v19.2R1-S4, 19.2R2, 19.3R2-S2, 19.3R3, 19.4R1-S1, 19.4R2, 20.1R1 ОС Junos Evolved до v19.4R2-EVO, 20.1R1-EVO
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 апреля 2020 г.
Дата обновления	15 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/JSA11019 https://nvd.nist.gov/vuln/detail/CVE-2020-1638