НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200611.3| 11 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в ОС Junos

Идентификатор уязвимости	MITRE: CVE-2020-1613
Идентификатор программной ошибки	CWE-710: Нарушение стандартов разработки кода
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально сформированного вредоносного сетевого пакета с BGP-сообщением NOTIFICATION. Уязвимость обусловлена некорректной работой BGP FlowSpec модуля.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	ОС Junos 12.3, 12.3X48, 14.1X53, 15.1, 15.1F, 15.1X49, 15.1X53, 16.1, 17.1, 17.2, 17.2X75, 17.3, 17.4, 18.1, 18.2X75.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 апреля 2020 г.
Дата обновления	13 апреля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/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)	Изменяется (C)

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/JSA10996 https://nvd.nist.gov/vuln/detail/CVE-2020-1613