НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN.20190531.2 | 31 мая 2019 г.

Уровень опасности: ВЫСОКИЙ

Уязвимость в обработке BGP-пакетов

Идентификатор уязвимости	MITRE: CVE-2019-0019 BDU: 2019-01661
Описание уязвимости	Злоумышленник может вызвать сбой или перезагрузку сервиса Routing protocol daemon (RPD) посредством отправки специально сформированных BGP-пакетов
Уязвимое ПО	JunOS версий 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2x75, 18.3 и 18.4.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	10 апреля 2019 г.
Дата обновления	15 апреля 2019 г.
Оценка критичности уязвимости	CVSSv3:7.5/AV:N/AC:L/PR:N/UI:N/S:U/E:X/RL:O
Вектор атаки	Сетевой
Сложность эксплуатации уязвимости	Низкая
Требуемый уровень привилегий	Отсутствует
Взаимодействие с пользователем	Нет
Влияние на другие компоненты системы	Не оказывает
Наличие эксплоита	Не определено
Средство устранения уязвимости	Официальное решение
Ссылки на источники	http://www.securityfocus.com/bid/107893 https://kb.juniper.net/JSA10931