НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190806.3 | 6 августа 2019 г.

Уровень опасности: ВЫСОКИЙ

Уязвимость протокола маршрутизации RPD в ОС Junos OS

Идентификатор уязвимости	MITRE: CVE-2019-0049 JUNIPER: JSA10943
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании оборудования посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной работой вспомогательного режима постепенного перезапуска BGP сессий.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	Junos OS до v18.4
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 июля 2019 г.
Дата обновления	25 июля 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.8 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:X/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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 (E)	Не определено (X)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки	https://nvd.nist.gov/vuln/detail/CVE-2019-0049 https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10943&actp=METADATA https://security-tracker.debian.org/tracker/CVE-2019-0049