НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201127.2 | 27 ноября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Juniper ОС Junos

Идентификатор уязвимости	MITRE: CVE-2020-1657
Идентификатор программной ошибки	CWE-408: Некорректный порядок действий: преждевременное расширение привилегий
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных IPv4 и IPv6 пакетов по протоколам IPSec. Уязвимость обусловлена некорректной работой службы менеджмента ключей (kmd), позволяющей сформировать IPv4 и IPv6 пакеты таким образом, чтобы они вызвали сбой в настройке канала IPSec.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Juniper Junos OS 12.3X48, 15.1X49, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1. Для платформ серии SRX.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 октября 2020 г.
Дата обновления	27 октября 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/JSA11050 https://nvd.nist.gov/vuln/detail/CVE-2020-1657