НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201127.5 | 27 ноября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в Juniper ОС Junos

Идентификатор уязвимости	MITRE: CVE-2020-1656
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных CWE-476: Разыменование нулевого указателя
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании или выполнить произвольный код в целевой системе посредством отправки специально сформированных DHCPv6 пакетов. Уязвимость обусловлена некорректной обработкой DHCPv6-пакетов сервисом DHCPv6 Relay-Agent. Если смежные устройства настроены на прозрачную ретрансляцию пакетов DHCPv6 вектор атаки может быть сетевым.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Juniper Junos OS 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2, 17.2X75, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 октября 2020 г.
Дата обновления	27 октября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Смежная сеть (A)
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)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
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/JSA11049 https://nvd.nist.gov/vuln/detail/CVE-2020-1656