НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210720.3 | 20 июля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости	MITRE: CVE-2021-0285
Идентификатор программной ошибки	CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки потока специально сформированных легитимных сетевых пакетов. Уязвимость обусловлена некорректным использованием внутренних ресурсов, приводящим к сбою работы Interchassis Control Protocol (ICCP).
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Juniper Junos OS в коммутаторах серии QFX5000 и EX4600: до v15.1R7-S9, 17.3R3-S11, 17.4R2-S13, 17.4R3-S5, 18.1R3-S13, 18.2R3-S8, 18.3R3-S5, 18.4R2-S8, 18.4R3-S7, 19.1R3-S5, 19.2R1-S6, 19.2R3-S2, 19.3R2-S6, 19.3R3-S2, 19.4R1-S4, 19.4R2-S4, 19.4R3-S2, 20.1R2-S2, 20.1R3, 20.2R2-S3, 20.2R3, 20.3R2, 20.4R1-S1, 20.4R2, 21.1R1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 июля 2021 г.
Дата обновления	19 июля 2021 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	Отсутствует (N)

пользователем (UI)	
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://www.cybersecurity-help.cz/vdb/SB2021071916 https://kb.juniper.net/JSA11187