НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211124.7 | 24 ноября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Juniper Networks Junos OS

Идентификатор уязвимости	MITRE: CVE-2021-31372
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику получить привилегии пользователя root в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Unix-подобные операционные системы и их компоненты
Уязвимый продукт	Juniper Networks Junos OS : от 12.3 до 12.3R12-S19, от 15.1 до 15.1R7-S10, от 18.3 до 18.3R3-S5, от 18.4 до 18.4R3-S9, от 19.1 до 19.1R3-S6, от 19.2 до 19.2R1-S7, 19.2R3-S3, от 19.3 до 19.3R3-S3, от 19.4 до 19.4R3-S5, от 20.1 до 20.1R2-S2, 20.1R3-S1, от 20.2 до 20.2R3-S2, от 20.3 до 20.3R3, от 20.4 до 20.4R2-S1, 20.4R3, От 21.1 до 21.1R1-S1, 21.1R2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 октября 2021 г.
Дата обновления	19 октября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
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://nvd.nist.gov/vuln/detail/CVE-2021-31372 https://kb.juniper.net/JSA11237