

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210423.1 | 23 апреля 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в ОС Junos

Идентификатор уязвимости	MITRE: CVE-2021-0254
Идентификатор программной ошибки	CWE: не определен
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных вредоносных сетевых пакетов по оверлейной сети. Уязвимость обусловлена некорректной обработкой входящих пакетов службой overlayd.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Junos OS 15.1X49, 15.1, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	20 апреля 2021 г.
Дата обновления	20 апреля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/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)	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/InfoCenter/index?page=content&id=SA11147&cat=SIRT_1&actp=LIST