

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220124.32 | 24 января 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Повышение привилегий в Juniper Junos OS J-Web

Идентификатор уязвимости	MITRE: CVE-2022-22162
Идентификатор программной ошибки	CWE-200: Разглашение важной информации лицам без соответствующих прав
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректным выводом данных.
Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	Juniper Junos OS: до 21.3R1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 января 2022 г.
Дата обновления	13 января 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
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://www.cybersecurity-help.cz/vdb/SB2022011314>
http://kb.juniper.net/InfoCenter/index?page=content&id=JS-A11270&cat=SIRT_1&actp=LIST