НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220114.14 | 14 января 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Juniper Junos OS FPC

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Juniper Junos OS: до 21.4R1
Дата выявления	12 января 2022 г.
Дата обновления	12 января 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-22170	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена утечкой памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-401: Некорректное освобождение памяти до удаления последней ссылки (утечка памяти) Рекомендации по устранению: обновить программное обеспечение	7.5

MITRE: CVE-2022-22171	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной обработкой ошибок. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-754: Некорректная проверка наличия нестандартных условий или исключений Рекомендации по устранению: обновить программное обеспечение	7.5

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2022011231 http://kb.juniper.net/InfoCenter/index?page=content&id=JSA11277&cat=SIRT_1&actp=LIST