НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201125.10 | 25 ноября 2020

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в библиотеке libfetch

Идентификатор уязвимости	MITRE: CVE-2020-7450
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного сетевого пакета. Уязвимость обусловлена некорректной работой программы с URL-адресами.
Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимый продукт	Библиотека передачи файлов libfetch используемая в FreeBSD: 12.1-STABLE до r357213, 12.1-RELEASE до 12.1-RELEASE-p2, 12.0-RELEASE до 12.0-RELEASE-p13, 11.3-STABLE до r357214 и 11.3-RELEASE до 11.3-RELEASE-p6; ОС Junos: 15.1, 17.2X75, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	18 февраля 2020 г.
Дата обновления	3 мая 2020 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://nvd.nist.gov/vuln/detail/CVE-2020-7450