НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201125.5| 25 ноября 2020

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Juniper ОС Junos

Идентификатор уязвимости	MITRE: CVE-2020-1673
Идентификатор программной ошибки	CWE-79: Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику разместить выполняемый вредоносный код в веб-странице целевой системы. Уязвимость обусловлена некорректной нейтрализацией входных данных в сервисе J-Web и веб-сервисах Juniper Networks (HTTP/HTTPS).
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Juniper Junos OS 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 октября 2020 г.
Дата обновления	29 октября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации	Не изменяется (U)

уязвимости (S)	
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/JSA11070 https://nvd.nist.gov/vuln/detail/CVE-2020-1673