НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200121.2 | 21 января 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Межсайтовый скриптинг в интерфейсе J-Web в ОС Junos OS

Идентификатор уязвимости	MITRE: CVE-2020-1607 Juniper: JSA10986
Идентификатор программной ошибки	CWE-79: Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику провести XSS атаку, в результате которой он может получить аутентификационные данные пользователя. Уязвимость обусловлена недостаточной очисткой вводимых пользователем данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Junos OS 12.3, 12.3X48, 14.1X53, 15.1, 15.1F6, 15.1X49, 15.1X53, 16.1, 16.2, 17.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 января 2020 г.
Дата обновления	16 января 2020 г.
Оценка критичности уязвимости (CVSSv3)	7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)

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 (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://kb.juniper.net/JSA10986 https://nvd.nist.gov/vuln/detail/CVE-2020-1607