НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191020.1 | 20 октября 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость проверки привилегий пользователя Junos OS

Идентификатор уязвимости	MITRE: CVE-2019-0073 Juniper: JSA10974 BDU: 2019-03834
Идентификатор программной ошибки	CWE-755: Некорректное назначение прав доступа для критических ресурсов
Описание уязвимости	Эксплуатация уязвимости позволяет авторизованному нарушителю получить несанкционированный доступ на чтение и изменение данных. Уязвимость обусловлена отсутствием проверки привилегий пользователя обращающегося к файлу криптографических ключей.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Junos OS версий 15.1X49-15.1X49-D180, 17.3-17.3R3-S7, 17.4-17.4R2-S8, 17.4R3, 18.1-18.1R3-S8, 18.2-18.2R3, 18.3-18.3R2, 18.4-18.4R2.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 октября 2019 г.
Дата обновления	20 октября 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.1 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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)	Отсутсвует (N)
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/JSA10974