НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191021.2 | 21 октября 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость подсистемы Veriexec Junos OS

Идентификатор уязвимости	MITRE: CVE-2019-0071 Juniper: JSA10978 BDU: 2019-03802
Идентификатор программной ошибки	CWE-269: Некорректное управление привилегиями CWE-347: Некорректная проверка криптографической подписи
Описание уязвимости	Эксплуатация уязвимости подсистемы Veriexec Junos OS позволяет локальному нарушителю повысить свои привилегии до администратора и перехватить управление системой посредством исполнения специально сформированного кода обновления прошивки.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Junos OS версии 18.1R3-S4 на коммутаторах EX2300, EX2300-C, EX3400 и версии 18.3R1-S3 на коммутаторах EX2300, EX2300-C and EX3400.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 октября 2019 г.
Дата обновления	21 октября 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/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)	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/JSA10978