НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200320.5| 20 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость в решении SD-WAN компании Cisco

Идентификатор уязвимости	MITRE: CVE-2020-3265
Идентификатор программной ошибки	CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить привилегии на целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Компоненты с версией ПО до 19.2.2: vBond Orchestrator Software vEdge 100 Series Routers vEdge 1000 Series Routers vEdge 2000 Series Routers vEdge 5000 Series Routers vEdge Cloud Router Platform vManage Network Management System vSmart Controller Software
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	18 марта 2020 г.
Дата обновления	18 марта 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.0 AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Высокая (H)

Необходимый уровень привилегий (PR)	Низкий (L)
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://www.cybersecurity-help.cz/vdb/SB2020031910?affChecked=1 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwpresc-ySJGvE9