НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210203.8 | 3 февраля 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Внедрение произвольных команд в Cisco DNA Center

Идентификатор уязвимости	MITRE: CVE-2021-1264
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (Внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированного вредоносного API-запроса на выполнение команды. Уязвимость обусловлена некорректной проверкой входящих запросов на выполнение команд с помощью инструмента Command Runner.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco DNA Center до v1.3.1.0.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	20 января 2021 г.
Дата обновления	27 января 2021 г.
Оценка критичности уязвимости (CVSSv3.0)	9.6 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)

Влияние на конфиденциальность (C)	Отсутствует (N)
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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-cmdinj-erumsWh9