

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200810.2 | 10 августа 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Раскрытие информации в Cisco DNA Center

Идентификатор уязвимости	MITRE: CVE-2020-3411
Идентификатор программной ошибки	CWE-200: Разглашение информации
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику осуществить НСД к данным файловой системы веб-сервисов на целевой системе посредством отправки специально сформированных HTTP-запросов. Уязвимость обусловлена некорректной обработкой аутентификационные токенов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco DNA Center все версии 1.3.x до 1.3.1.4
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 августа 2020 г.
Дата обновления	5 августа 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
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)	Отсутствует (N)

Влияние на доступность (A)

Отсутствует (N)

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-dna-info-disc-3bz8BCgR>