

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210618.1 | 18 июня 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Уязвимость при проверке сертификатов в Cisco DNA Center

Идентификатор уязвимости	MITRE: CVE-2021-1134
Идентификатор программной ошибки	CWE-295: Некорректная проверка сертификатов
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить несанкционированный доступ к данным в целевой системе посредством отправки специально созданных сетевых пакетов. Уязвимость обусловлена некорректной проверкой сертификата X.509.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco DNA Center до v2.2.2.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 июня 2021 г.
Дата обновления	16 июня 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.4 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
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)	Высокое (H)

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-dnac-certvalid-USEj2CZk>