НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210827.5 | 27 августа 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco Nexus серии 9000

Идентификатор уязвимости	MITRE: CVE-2021-1586
Идентификатор программной ошибки	CWE-345: Некорректная проверка достоверности данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной проверкой TCP пакетов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Nexus 9000 Series Switches: 15.0(2e), 15.1(1h)
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	26 августа 2021 г.
Дата обновления	26 августа 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
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)	Изменяется (C)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)

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/SB2021082603 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9kaci-tcp-dos-YXukt6gM