

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200810.3 | 10 августа 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Отказ в обслуживании в ПО Cisco StarOS IPv6

Идентификатор уязвимости	MITRE: CVE-2020-3324
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного сетевого пакета IPv6. Уязвимость обусловлена некорректной проверкой входящих IPv6-пакетов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco StarOS 21.15, 21.16, 21.16.c, 21.16.d, 21.17, 21.18, 21.19
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 августа 2020 г.
Дата обновления	5 августа 2020 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr-dos-zLJFgBf>