# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210203.7 | 3 февраля 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

## Выполнение произвольного кода в Cisco SD-WAN

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2021-1300 |
| Идентификатор программной ошибки | CWE-119: Выполнение операций за пределами буфера памяти |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного IP-трафика. Уязвимость обусловлена некорректной проверкой входящего IP-трафика. |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимый продукт | Релизы Cisco SD-WAN ранее v18,3, 18,3, 18,4, 19,2, 19,3, 20,1, 20,3, 20,4<br>Релизы Cisco IOS XE SD-WAN 16.9, 16.10, 16.11, 16.12<br>Релизы Cisco IOS XE Universal 17,2, 17,3, 17,4 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 20 января 2021 г. |
| Дата обновления | 20 января 2021 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/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) | Не изменяется (U) |

| | |
|---|---|
| Влияние на конфиденциальность (C) | Высокое (H) |
| 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-sdwan-bufovulns-B5NrSHbj |