

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211102.1 | 2 ноября 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольных команд оболочки в Cisco IOS XE SD-WAN

Идентификатор уязвимости	MITRE: CVE-2021-1529
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольные команды оболочки с привилегиями пользователя root в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco IOS XE SD-WAN: 17.2, 17.3, 17.4, 17.5, 17.6 Cisco 1000 Series Integrated Services Routers: все версии 4000 Series Integrated Services Routers: все версии Cisco ASR 1000 Series Aggregation Services Routers: все версии Catalyst 8000V Edge Software: все версии Cloud Services Router 1000V Series: все версии
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	21 октября 2021 г.
Дата обновления	21 октября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)

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://www.cybersecurity-help.cz/vdb/SB2021102131 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A