НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200907.4| 7 сентября 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Cisco SD-WAN

Идентификатор уязвимости	MITRE: CVE-2020-3374 CVE-2020-3375
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии, получить НСД к данным, внести изменения в систему и выполнить команды с привилегиями пользователя root в уязвимой системе посредством отправки специально созданных вредоносных сетевых пакетов. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	IOS XE SD-WAN до v17.2.1r SD-WAN vBond, SD-WAN vEdge, SD-WAN vManage, SD-WAN vSmart до v20.1.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	29 июля 2020 г.
Дата обновления	29 июля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.9 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-uabvman-SYGzt8Bv https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdbufof-h5f5VSeL