НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200123.1 | 23 января 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Внедрение команд в ПО Cisco Data Center Network Manager (DCNM)

Идентификатор уязвимости	MITRE: CVE-2019-15978 CVE-2019-15979 Cisco: cisco-sa-20200102-dcnm-comm-inject
Идентификатор программной ошибки	CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)
Описание уязвимости	Эксплуатация любой из уязвимостей позволяет удаленному злоумышленнику с привилегиями администратора в приложении DCNM выполнить произвольные команды в хостовой операционной системе посредством отправки специально созданного вредоносного запроса. Уязвимость обусловлена некорректной проверкой введенных пользователем данных в API.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco DCNM до v.11.3(1)
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	2 января 2020 г.
Дата обновления	15 января 2020 г.
Оценка критичности уязвимости (CVSSv3)	9.8 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Высокий (H)
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 (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200102-dcnm-comm-inject