НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200121.5 | 21 января 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Обход аутентификации в ПО Cisco Data Center Network Manager (DCNM)

Идентификатор уязвимости	MITRE: CVE-2019-15975 CVE-2019-15976 CVE-2019-15977 Cisco: cisco-sa-20200102-dcnm-auth-bypass
Идентификатор программной ошибки	CWE-798: Использование жестко закодированных учетных данных
Описание уязвимости	Эксплуатация любой из уязвимостей позволяет удаленному злоумышленнику выполнить произвольные действия с правами администратора в целевой системе. Уязвимость обусловлена некорректной работой механизма аутентификации.
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:N/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)	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 (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-auth-bypass