# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200312.6 | 12 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Повышение привилегий в платформе Cisco Data Center Network Manager

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2019-3112 |
| Идентификатор программной ошибки | CWE-20: Некорректная проверка входных данных |
| Описание уязвимости | Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированного запроса при использовании REST API. Уязвимость обусловлена некорректным определением привилегий обрабатываемых API запросов. |
| Категория уязвимого продукта | Серверное программное обеспечение и его компоненты |
| Уязвимое ПО | Cisco DCNM v11.3(1) и более поздниии версии |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 30 января 2020 г. |
| Дата обновления | 31 января 2020 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/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) | Изменяется (C) |
| Влияние на конфиденциальность (C) | Отсутствует (N) |
| Влияние на целостность (I) | Отсутствует (N) |

| | |
|---|---|
| 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-20200219-dcnm-priv-esc<br>https://nvd.nist.gov/vuln/detail/CVE-2020-3112 |