НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210203.11 | 3 февраля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Data Center Network Manager

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Релизы Cisco DCNM ранее 11.5(1)
Дата выявления	20 января 2021 г.
Дата обновления	20 января 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-1272	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированных HTTP-пакетов. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-918: Подделка запроса со стороны сервера Рекомендации по устранению: обновить программное обеспечение.	8.8

MITRE: CVE-2021-1247	Эксплуатация уязвимости позволяет удаленному авторизованному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированных API-запросов. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (Внедрение SQL-кода) Рекомендации по устранению: обновить программное обеспечение.	8.8
MITRE: CVE-2021-1248	Эксплуатация уязвимости позволяет удаленному авторизованному как администратору злоумышленнику получить НСД к целевой системе посредством отправки специально сформированных API-запросов. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-89: Некорректная нейтрализация специальных элементов, используемых в SQL-командах (Внедрение SQL-кода) Рекомендации по устранению: обновить программное обеспечение.	7.2

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-ssrf-F2vX6q5p https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dcnm-sql-inj-OAQOObP