НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210514.3 | 14 мая 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco SD-WAN vManage

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco SD-WAN vManage v18.4 и ранее, 19.2, 20.1, 20.3, 20.4, 20.5
Дата выявления	5 мая 2021 г.
Дата обновления	5 мая 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-1468	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации в целевой системе и выполнить произвольные действия посредством отправки специально сформированного вредоносного сообщения. Уязвимость обусловлена некорректной проверкой входящих сообщений в службе обмена сообщениями при работе в кластерном режиме. CVSSv3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-287: Некорректная аутентификация Рекомендации по устранению: обновить программное обеспечение.	9.8

MITRE: CVE-2021-1505	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входящих запросов в кластерном режиме. CVSSv3.0: AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение.	9.1
MITRE: CVE-2021-1508	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику изменить конфигурацию и повысить свои привилегии в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входящих запросов в кластерном режиме. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: обновить программное обеспечение.	8.1
MITRE: CVE-2021-1275	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки множественных API-запросов. Уязвимость обусловлена некорректной обработкой входящих API-запросов. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	7.5

MITRE: CVE-2021-1506	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику получить несанкционированный доступ к службам в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной обработкой входящих запросов в кластерном режиме. 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-284: Некорректное управление доступом Рекомендации по устранению: обновить программное обеспечение.	7.2

Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-4TbynnhZ https://www.cybersecurity-help.cz/vdb/SB2021050616