

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210527.3 | 27 мая 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Уязвимость в веб-интерфейсе Cisco HyperFlex HX

| | |
|---|--|
| Идентификатор уязвимости | MITRE: CVE-2021-1497 |
| Идентификатор программной ошибки | CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе с правами администратора посредством отправки специально сформированных запросов в веб-интерфейс управления. Уязвимость обусловлена некорректной проверкой вводимых данных. |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимый продукт | HyperFlex HX: 4.0, 4.5 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 6 мая 2021 г. |
| Дата обновления | 6 мая 2021 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/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) | 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 | Наличие не подтверждено |
| Наличие средств устранения уязвимости | Официальное решение |
| Достоверность сведений об уязвимости | Сведения подтверждены |

| | |
|---------------------|--|
| Ссылки на источники | https://www.cybersecurity-help.cz/vdb/SB2021050629 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR |
|---------------------|--|