НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220224.7 | 24 февраля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco NX-OS Fabric Services Over IP feature

Идентификатор уязвимости	MITRE: CVE-2022-20624
Идентификатор программной ошибки	CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена некорректным использованием ресурсов.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Cisco NX-OS: до 9.3(8) Cisco UCS: до 4.2(1l)
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	24 февраля 2022 г.
Дата обновления	24 февраля 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/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)	Не изменяется (U)
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://www.cybersecurity-help.cz/vdb/SB2022022402 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cfsoip-dos-tpykyDr http://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy95696 http://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy95840