НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200522.14| 22 мая 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в продуктах компании Cisco с ПО Cisco NX-OS

Идентификатор уязвимости	MITRE: CVE-2020-3175
Идентификатор программной ошибки	CWE-664: Некорректное обращение с ресурсом на протяжении его жизненного цикла
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки большого количества пакетов на интерфейс управления (mgmt0) уязвимого устройства. Уязвимость обусловлена некорректным контролем использования ресурсов.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	Cisco NX-OS на следующих продуктах: MDS 9100 Series Multilayer Fabric Switches, MDS 9250i Multiservice Fabric Switches, MDS 9300 Series Multilayer Fabric Switche.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	26 февраля 2020 г.
Дата обновления	21 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
Вектор атаки (AV)	Удаленный (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-20200226-mds-ovrld-dos