НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210419.2 | 19 апреля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в продуктах компании Cisco

Идентификатор уязвимости	MITRE: CVE-2021-1352
Идентификатор программной ошибки	CWE-823: Использование для указателя смещения за пределами назначенного диапазона
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально созданного вредоносного DECnet-пакета. Уязвимость обусловлена некорректной проверкой DECnet-пакетов.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco 2600 Series Multiservice Platforms Cisco ASR 1000 Series Aggregation Services Routers Cisco Cloud Services Router 1000V Series Cisco Catalyst 3850 Series Switches Cisco Catalyst 3650 Series Switches Cisco 4000 Series Integrated Services Routers Cisco 1000 Series Integrated Services Routers Cisco Catalyst 9300 Series Switches Cisco Catalyst 9500 Series Switches Cisco Catalyst 9400 Series Switches Cisco 1100 Series Industrial Integrated Services Routers Cisco Catalyst 9200 Series Switches Cisco Embedded Services 3300 Series Switches Cisco Catalyst IE3200 Rugged Series Cisco Catalyst IE3300 Rugged Series Cisco Catalyst IE3400 Rugged Series Cisco Catalyst 9600 Series Switches Cisco Catalyst 9800 Series Wireless Controllers Cisco Catalyst IE3400 Heavy Duty Series Cisco IOS XE:16.12

Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	24 марта 2021 г.
Дата обновления	24 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.4 AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
Вектор атаки (AV)	Смежная сеть (A)
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://www.cybersecurity-help.cz/vdb/SB2021032417 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-decnet-dos-cuPWDkyL https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvv51476