НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200207.3 | 7 февраля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании устройств компании Cisco

Идентификатор уязвимости	MITRE: CVE-2020-3120 Cisco: cisco-sa-20200205-fxnxos-iosxr-cdp-dos
Идентификатор программной ошибки	CWE-190: Целочисленное переполнение или циклический возврат
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании оборудования целевой системы посредством отправки вредоносного пакета Cisco Discovery Protocol. Уязвимость обусловлена некорректной проверкой при обработке сообщений.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	ASR 9000 Series Aggregation Services Routers Carrier Routing System (CRS) Firepower 4100 Series Firepower 9300 Security Appliances IOS XRv 9000 Router MDS 9000 Series Multilayer Switches Network Convergence System (NCS) 540 Series Routers Network Convergence System (NCS) 560 Series Routers Network Convergence System (NCS) 1000 Series Network Convergence System (NCS) 5000 Series Network Convergence System (NCS) 5500 Series Network Convergence System (NCS) 6000 Series Nexus 1000 Virtual Edge for VMware vSphere Nexus 1000V Switch for Microsoft Hyper-V Nexus 1000V Switch for VMware vSphere Nexus 3000 Series Switches Nexus 5500 Platform Switches Nexus 5600 Platform Switches Nexus 6000 Series Switches

	Nexus 7000 Series Switches Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode Nexus 9000 Series Switches in standalone NX-OS mode UCS 6200 Series Fabric Interconnects UCS 6300 Series Fabric Interconnects UCS 6400 Series Fabric Interconnects
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 февраля 2020 г.
Дата обновления	5 февраля 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	7.4 AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:U/RL:O/RC:C
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 (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos https://www.armis.com/cdpwn/