НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200605.2| 5 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco NX-OS

Идентификатор уязвимости	MITRE: CVE-2020-10136
Идентификатор программной ошибки	CWE-19: Ошибки, связанные с обработкой данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного вредоносного сетевого пакета с определенным IP-адресом. Уязвимость обусловлена некорректной обработкой IP-адреса в сетевых пакетах.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Nexus 1000 Virtual Edge для VMware vSphere (CSCvu10050) Nexus 1000V Switch для Microsoft Hyper-V (CSCvt67738) Коммутатор Nexus 1000 B для VMware vSphere (CSCvt67738) Коммутаторы Nexus серии 3000 (CSCun53663) 1 Коммутаторы платформы Nexus 5500 (CSCvt67739) Коммутаторы платформы Nexus 5600 (CSCvt67739) Коммутаторы Nexus серии 6000 (CSCvt67739) Коммутаторы серии Nexus 7000 (CSCvt66624) Коммутаторы серии Nexus 9000 в автономном режиме NX-OS (CSCun53663) UCS 6200 Series Fabric Interconnects (CSCvu03158) UCS 6300 Series Fabric Interconnects (CSCvt67740)
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	1 июня 2020 г.
Дата обновления	2 июня 2020 г.

Оценка критичности уязвимости (CVSSv3.1)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/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)	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-nxos-ipip-dos-kCT9X4