НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211008.5 | 8 октября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Cisco Small Business 220 Series Smart Switches

Идентификатор уязвимости	MITRE: CVE-2021-34780 CVE-2021-34779
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти при обработке сообщений LLDP в протоколе обнаружения канального уровня.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Small Business 220 Series Smart Switches: 1.2.0.6
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	7 октября 2021 г.
Дата обновления	7 октября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/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)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)

Влияние на целостность (I)	Высокое (H)
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/SB2021100710 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T