НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210618.2 | 18 июня 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Несанкционированный доступ в Cisco Small Business

Идентификатор уязвимости	MITRE: CVE-2021-1542
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти процесс аутентификации и получить несанкционированный доступ к интерфейсу уязвимого приложения посредством создания действительного идентификатора сеанса. Уязвимость обусловлена ошибкой в управлении сеансом.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Small Business 220 Series Smart Switches: до v1.2.0.6
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 июня 2021 г.
Дата обновления	16 июня 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
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/SB2021061622 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvx57925