НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211108.2 | 8 ноября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Несанкционированный доступ в коммутаторах Cisco Small Business Series

Идентификатор уязвимости	MITRE: CVE-2021-34739
Идентификатор программной ошибки	CWE-613: Некорректно настроенный срок действия сессий
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к веб-интерфейсу управления целевого устройства посредством перехвата действительных учетный данных сеанса. Уязвимость обусловлена некорректным истечением срока действия учетных данных сеанса.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco 250 Series Smart Switches: все версии Cisco 350 Series Managed Switches: все версии Cisco 350X Series Stackable Managed Switches: все версии Cisco 550X Series Stackable Managed Switches: все версии Business 250 Series Smart Switches: все версии Business 350 Series Managed Switches: все версии Cisco ESW2 Series Advanced Switches: все версии Cisco Small Business 200 Series Smart Switches: все версии Cisco Small Business 300 Series Managed Switches: все версии Cisco Small Business 500 Series Stackable Managed Switches: все версии
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	4 ноября 2021 г.
Дата обновления	4 ноября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.1 AV:N/AC:H/PR:N/UI:N/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)	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/SB2021110416 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-switches-tokens-UzwpR4e5