НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210419.4 | 19 апреля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Cisco IOS и Cisco IOS XE

Идентификатор уязвимости	MITRE: CVE-2021-1392
Идентификатор программной ошибки	CWE-522: Недостаточно надежная защита учетных данных
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику получить привилегии администратора и изменить настойки устройства посредством выполнения команды в командной строке и получения пароля для доступа по протоколу CIP. Уязвимость обусловлена некорректной работой команды «show cip security» в командной строке.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco IOS: 17.1.1 Cisco IOS XE: 17.1.1 Cisco Embedded Services 3300 Series Switches
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	29 марта 2021 г.
Дата обновления	29 марта 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
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/SB2021032917 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-XE-SAP-OPLbze68