НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200207.6 | 7 февраля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость к CSRF атаке в ПО Cisco IOS

Идентификатор уязвимости	MITRE: CVE-2019-16009 Cisco: cisco-sa-20200108-ios-csrf
Идентификатор программной ошибки	CWE-352: Подделка межсайтового запроса
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в приложении с уровнем привилегий целевого пользователя посредством перехода этим пользователем по вредоносной ссылке. Уязвимость обусловлена недостаточной защитой веб-интерфейса от CSRF-атак.
Категория уязвимого продукта	Телекоммуникационные оборудование
Уязвимое ПО	Cisco IOS v16.1.1 и ранее Cisco IOS XE v16.1.1 и ранее
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 января 2020 г.
Дата обновления	8 января 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
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 (E)	Наличие не подтверждено (U)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200108-ios-csrf