НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201027.12 | 27 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Межсайтовая подделка запросов в ПО Cisco FXOS

Идентификатор уязвимости	MITRE: CVE-2020-3456
Идентификатор программной ошибки	CWE-352: Подделка межсайтового запроса (CSRF)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить несанкционированные действия на уязвимом устройстве посредством проведения CSRF-атаки (межсайтовой подделки запросов) после открытия пользователем специально созданной вредоносной ссылки. Уязвимость обусловлена некорректной защитой от CSRF-атак в интерфейсе Firepower Chassis Manager (FCM).
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	ПО Cisco FXOS на следующих платформах: Firepower 2100 при запуске ПО ASA в режиме non-appliance; Firepower 4100; Firepower 9300.
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	21 октября 2020 г.
Дата обновления	21 октября 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
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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxosfcm-csrf-uhO4e5BZ