НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201030.8 | 30 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Несанкционированный доступ в ПО Cisco FMC и FTD

Идентификатор уязвимости	MITRE: CVE-2020-3549
Идентификатор программной ошибки	CWE-326: Недостаточно надежное шифрование
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить регистрационный хэш целевого устройства посредством перехвата определенных сетевых пакетов между устройствами с уязвимым ПО. Уязвимость обусловлена некорректной защитой сетевого согласования во время первоначальной регистрации устройства.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	ПО Cisco FMC и FTD до v6.6.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	21 октября 2020 г.
Дата обновления	21 октября 2020 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)	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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftdfmc-sft-mitm-tc8AzFs2