НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210716.2 | 16 июля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco Adaptive Security Appliance и Firepower Threat Defense

Идентификатор уязвимости	MITRE: CVE-2021-1422
Идентификатор программной ошибки	CWE-617: Несанкционированный вызов утверждения
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных вредоносных сетевых пакетов через установленное соединение IPsec. Уязвимость обусловлена некорректной работой криптографического модуля при обработке входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco ASA v9.16.1 Cisco FTD v7.0.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	15 июля 2021 г.
Дата обновления	15 июля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)

Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)
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-asa-ftd-ipsec-dos-TFKQbgWC