НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210430.10 | 30 апреля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Переполнение буфера в Cisco ASA и FTD

Идентификатор уязвимости	MITRE: CVE-2021-1493
Идентификатор программной ошибки	CWE-120: Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику вызвать отказ в обслуживании или получить доступ к части информации в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной обработкой входящих запросов службами веб-интерфейса.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Adaptive Security Appliance (ASA) Software: до v9.8.4.35, 9.9.2.85, 9.12.4.18, 9.13.1.2, 9.14.2.13, 9.15.1.15 Cisco Firepower Threat Defense (FTD) Software: до v6.4.0.12, 6.6.4, 6.7.0.2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	28 апреля 2021 г.
Дата обновления	28 апреля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.5 AV:N/AC:L/PR:L/UI:N/S:C/C:L/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)	Низкое (L)
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-memc-dos-fncTyYKG