НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200810.7| 10 августа 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость в веб-интерфейсе Cisco ASA и Cisco FTD

Идентификатор уязвимости	MITRE: CVE-2020-3452
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику осуществить НСД к данным файловой системы веб-сервисов на целевой системе посредством отправки специально сформированных HTTP-запросов. Уязвимость обусловлена некорректной обработкой входных данных компонентами WebVPN и AnyConnect.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	Cisco ASA Software до версии 9.14 включительно, исключая версию 9.11 Cisco FTD Software до версии 6.2.2 включительно, и 6.2.3,6.3.0,6.4.0,6.50,6.60
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 июля 2020 г.
Дата обновления	28 июля 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации	Не изменяется (U)

уязвимости (S)	
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Отсутствует (N)
Влияние на доступность (A)	Отсутствует (N)
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-asaftd-ro-path-KJuQhB86