



НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)  
E-mail: [gov-cert@gov-cert.ru](mailto:gov-cert@gov-cert.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN.20190619.5 | 19 июня 2019 г.

Уровень опасности: **Высокий**

## Уязвимость реализации протокола TCP межсетевых экранов Cisco ASA и Cisco FTD

Идентификатор уязвимости	MITRE: CVE-2019-1694 BDU: 2019-01790
Описание уязвимости	Уязвимость реализации протокола TCP позволяет злоумышленнику вызвать отказ в обслуживании оборудования посредством отправки последовательности специально сформированных сетевых пакетов с высокой скоростью через уязвимое устройство
Уязвимое ПО	Cisco ASA версий 9.9 - 9.9.2.50, 9.10 - 9.10.1.17, 9.5 - 9.6.4.25, 9.7 - 9.8.4, 9.4 - 9.4.4.34 Cisco FTD 6.3.0 - 6.3.0.3, 6.0 - 6.2.3.12
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	03 мая 2019 г.
Дата обновления	07 мая 2019 г.
Оценка критичности уязвимости	CVSSv3:8.6/AV:N/AC:L/PR:N/UI:N/S:C
Вектор атаки	Сетевой
Сложность эксплуатации уязвимости	Низкая
Требуемый уровень привилегий	Отсутствует
Взаимодействие с пользователем	Нет
Влияние на другие компоненты системы	Оказывает
Наличие эксплоита	Не определено
Средство устранения уязвимости	Официальное решение

Ссылки на источники

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-asa-frpwrtd-dos>