НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20190712.3 | 12 июля 2019 г.

Уровень опасности: ВЫСОКИЙ

Уязвимость драйвера МЭ Cisco Adaptive Security Appliance (ASA)

Идентификатор уязвимости	CISCO: cisco-sa-20190710-asa-ftd-dos MITRE: CVE-2019-1873
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально сформированного сетевого TLS/SSL-пакета. Уязвимость обусловлена неполной проверкой заголовка сетевого пакета криптографических протоколов TLS/SSL.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимые системы и программное обеспечение	ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	10 июля 2019 г.
Дата обновления	10 июля 2019 г.
Оценка критичности уязвимости (CVSSv3)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:X/RL:O/RC:X
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Не требуется (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 (E)	Не определено (X)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Не определено (X)
Ссылки	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190710-asa-ftd-dos