

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN.20190619.3 | 19 июня 2019 г.

Уровень опасности: **ВЫСОКИЙ**

Уязвимость прокси-сервера ОС Cisco AsyncOS интернет-шлюзов Cisco Web Security Appliance

Идентификатор уязвимости	MITRE: CVE-2019-1817 BDU: 2019-01787
Описание уязвимости	Уязвимость позволяет злоумышленнику вызвать отказ в обслуживании оборудования в результате отправки на уязвимое устройство специально сформированного HTTP или HTTPS запроса
Уязвимое ПО	Cisco WSA версий 11.5.1-fcs-115, 11.5.1-fcs-124, 11.5.1-fcs-125 и 11.7.0-fcs-334
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	03 мая 2019 г.
Дата обновления	06 мая 2019 г.
Оценка критичности уязвимости	CVSSv3:7.5/AV:N/AC:L/PR:N/UI:N/S:U
Вектор атаки	Сетевой
Сложность эксплуатации уязвимости	Низкая
Требуемый уровень привилегий	Отсутствует
Взаимодействие с пользователем	Нет
Влияние на другие компоненты системы	Не оказывает
Наличие эксплоита	Не определено
Средство устранения уязвимости	Официальное решение
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-wsa-dos