

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201030.12 | 30 октября 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Отказ в обслуживании в Cisco Adaptive Security Appliance Software

Идентификатор уязвимости	MITRE: CVE-2020-27124
Идентификатор программной ошибки	CWE-457: Использование неинициализированной переменной
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы путем отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной обработкой ошибок при функционировании модуля SSL/TLS.
Категория уязвимого продукта	Средства защиты информации
Уязвимый продукт	Cisco ASA Software: 9.13.1.12, 9.13.1.13, 9.14.1.10
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	22 октября 2020 г.
Дата обновления	27 октября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
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 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

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-asa-ssl-dos-7uZWwSEy>