НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211119.14 | 19 ноября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в Cisco Adaptive Security Appliance (ASA) Software

Идентификатор уязвимости	MITRE: CVE-2021-40117
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTPS-запроса. Уязвимость обусловлена ошибкой границ памяти при обработке пакетов SSL/TLS в интерфейсе SSL VPN.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco Adaptive Security Appliance (ASA) Software: 9.7, 9.8, 9.8.4.3, 9.8.4.7, 9.8.4.10, 9.8.4.12, 9.8.4.15, 9.8.4.17, 9.8.4.20, 9.8.4.22, 9.8.4.25, 9.8.4.26, 9.8.4.29, 9.8.4.35, 9.9, 9.9.2.52, 9.9.2.66, 9.9.2.67, 9.9.2.74, 9.9.2.80, 9.9.2.85, 9.10, 9.10.1.22, 9.10.1.27, 9.10.1.30, 9.10.1.37, 9.10.1.39, 9.10.1.42, 9.10.1.43, 9.10.1.44, 9.12, 9.12.2, 9.12.2.1, 9.12.2.9, 9.12.3, 9.12.3.2, 9.12.3.7, 9.12.3.9, 9.12.3.12, 9.12.4.2, 9.12.4.3, 9.12.4.4, 9.12.4.13, 9.12.4.18, 9.12.4.24, 9.13, 9.13.1.2, 9.13.1.7, 9.13.1.10, 9.13.1.12, 9.13.1.13, 9.13.1.21, 9.14, 9.14.1.10, 9.14.1.15, 9.14.1.19, 9.14.1.30, 9.14.2.8, 9.14.2.13, 9.14.2.15, 9.14.3, 9.15.1.7, 9.15.1.10, 9.15.1.15 ASA 5500-X Series Firewalls: все версии Cisco Firepower Threat Defense (FTD): 6.2.2, 6.2.2.1, 6.2.3, 6.2.3.4, 6.2.3.12, 6.2.3.13, 6.2.3.15, 6.2.3.16, 6.3.0, 6.3.0.2, 6.3.0.4, 6.3.0.5, 6.3.0.6, 6.4.0, 6.4.0.2, 6.4.0.3, 6.4.0.4, 6.4.0.6, 6.4.0.7, 6.4.0.8, 6.4.0.10, 6.4.0.12, 6.5.0, 6.5.0.2, 6.5.0.3, 6.5.0.4, 6.5.0.5, 6.6.0, 6.6.0.1, 6.6.1, 6.6.4, 6.7.0, 6.7.0.1, 6.7.0.2

Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	28 октября 2021 г.
Дата обновления	28 октября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:L/PR:N/UI:N/S:U/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)	Не изменяется (U)
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://www.cybersecurity-help.cz/vdb/SB2021102806 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9 http://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy43187