НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211125.1 | 25 ноября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco Adaptive Security Appliance (ASA) Software

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, 9.15.1.7, 9.15.1.10, 9.15.1.15, 9.16 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, 7.0.0
Дата выявления	28 октября 2021 г.
Дата обновления	28 октября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS

MITRE: CVE-2021-1573	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена ошибкой границ памяти при обработке HTTP-запросов, отправленных на интерфейс SSL VPN. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2021-34704	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных при обработке HTTP-запросов, отправленных на интерфейс SSL VPN. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение	7.5
MITRE: CVE-2021-40118	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена ошибкой границ памяти при обработке HTTP-запросов, отправленных на интерфейс SSL VPN. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение	7.5

Ссылки на источники	http://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy58278 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA https://www.cybersecurity-help.cz/vdb/SB2021102805 http://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy89144 http://bst.cloudapps.cisco.com/bugsearch/bug/CSCvy36910