НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220516.13 | 16 мая 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Cisco ASA and Cisco FTD

Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	Cisco ASA: до 9.17.1.7, 9.16.2.14, 9.15.1.21, 9.14.4, 9.12.4.38 Cisco Firepower Threat Defense (FTD): 7.0.0 - 7.0.1, 6.7.0 - 6.7.0.3, 6.6.0 - 6.6.5, 6.5.0 - 6.5.0.5, 6.4.0 - 6.4.0.12, 6.3.0 - 6.3.0.6, 6.2.3 - 6.2.3.17, 6.2.2 - 6.2.2.1
Дата выявления	27 апреля 2022 г.
Дата обновления	27 апреля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-20760	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных DNS-запросов. Уязвимость обусловлена некорректным управлением внутренними ресурсами. 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-400: Неконтролируемое использование ресурсов (исчерпание ресурсов) Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	7.5

MITRE: CVE-2022-20745	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных HTTP-запросов. Уязвимость обусловлена некорректной проверкой входных данных. 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: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	7.5

Ссылки на источники	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-nJVAwOeq http://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz76966 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-tzPSYern http://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz70595