НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191122.3 | 22 ноября 2019 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Уязвимость обработки LSA в ПО межсетевых экранов Cisco.

Идентификатор уязвимости	MITRE: CVE-2019-12676 Cisco: cisco-sa-20191002-asa-ospf-lsa-dos BDU: 2019-03707
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет злоумышленнику вызвать отказ обслуживания в целевой системе посредством отправки специально созданного пакета OSPF LSA type 11. Уязвимость обусловлена некорректной обработкой параметров пакета OSPF LSA type 11.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	Cisco ASA Software 9.4.1 Cisco ASA Software 9.5.1 Cisco ASA Software 9.6 Cisco ASA Software 9.7.1 Cisco ASA Software 9.8 Cisco ASA Software 9.9 Cisco ASA Software 9.10 Cisco ASA Software 9.12 Cisco FTD 6.1.0 Cisco FTD 6.2.0 Cisco FTD 6.2.1 Cisco FTD 6.2.2 Cisco FTD 6.2.3 Cisco FTD 6.3.0 Cisco FTD 6.4.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	27 сентября 2019 г.

Дата обновления	10 октября 2019 г.
Оценка критичности уязвимости (CVSSv3)	7.4 AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:U/RC:C
Вектор атаки (AV)	Смежная сеть (A)
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 (E)	Концептуальное подтверждение (P)
Наличие средств устранения уязвимости (RL)	Недоступно (U)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ospf-lsa-dos https://nvd.nist.gov/vuln/detail/CVE-2019-12676 https://www.symantec.com/security-center/vulnerabilities/writeup/110311