НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200513.12| 13 мая 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Уязвимость отказа в обслуживании в Cisco Firepower 1000 Series

Идентификатор уязвимости	MITRE: CVE-2020-3283
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевого устройства посредством отправки специально созданного сетевого пакета SSL/TLS. Уязвимость обусловлена некорректной реализацией внутренних функций механизма обработки SSL/TLS соединений.
Категория уязвимого продукта	Коммуникационное оборудование
Уязвимое ПО	Cisco Firepower 1000 Series с программным обеспечением Cisco Firepower Threat Defense
Рекомендации по устранению	На данный момент отсутствуют
Дата выявления	6 мая 2020 г.
Дата обновления	6 мая 2020 г.
Оценка критичности уязвимости (CVSSv3.0)	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	Отсутствует
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-dos-4v5nmWtZ https://www.cybersecurity-help.cz/vdb/SB2020051141