НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200617.4| 17 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Отказ в обслуживании в маршрутизаторе TP-Link Archer C50 V3

Идентификатор уязвимости	MITRE: CVE-2020-9375
Идентификатор программной ошибки	CWE-772: Удержание ресурса после его использования
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного вредоносного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое ПО	TP-Link Archer C50 V3 с ПО до версии 200318
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	25 марта 2020 г.
Дата обновления	31 марта 2020 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	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2020-9375 https://thewhiteh4t.github.io/2020/02/27/CVE-2020-9375-TP-Link-Archer-C50-v3-Denial-of-Service.html