НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200207.7 | 7 февраля 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Переполнение буфера в маршрутизаторе TP-Link

Идентификатор уязвимости	MITRE: CVE-2019-17147 ZDI: ZDI-CAN-8457
Идентификатор программной ошибки	CWE-120: Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код на целевом устройстве посредством отправки специально сформированного вредоносного http-запроса. Уязвимость обусловленная некорректной работой веб-службы при проверке предоставленных пользователем данных.
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимое оборудование	TP-Link TL-WR841N
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	7 января 2020
Дата обновления	14 января 2020
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (U)

Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации (E)	Функциональная версия (F)
Наличие средств устранения уязвимости (RL)	Официальное решение (O)
Достоверность сведений об уязвимости (RC)	Сведения подтверждены (C)
Ссылки на источники	https://www.tp-link.com/us/support/download/tl-wr841n/#Firmware https://www.zerodayinitiative.com/advisories/ZDI-19-992/ https://amonitoring.ru/article/CVE-2019-17147/