# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211130.2 | 30 ноября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

## Выполнение произвольного кода в TP-Link TL-XVR1800L

| | |
|---|---|
| Идентификатор уязвимости | Не определен |
| Идентификатор программной ошибки | CWE-94: Некорректное управление генерированием кода (внедрение кода) |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных. |
| Категория уязвимого продукта | Телекоммуникационное оборудование |
| Уязвимый продукт | TL-XVR1800L: все версии |
| Рекомендации по устранению | Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами |
| Дата выявления | 29 ноября 2021 г. |
| Дата обновления | 29 ноября 2021 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/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) | Высокое (H) |

| | |
|---|---|
| Влияние на целостность (I) | Высокое (H) |
| Влияние на доступность (A) | Высокое (H) |
| Степень зрелости доступных средств эксплуатации | Наличие не подтверждено |
| Наличие средств устранения уязвимости | Недоступно |
| Достоверность сведений об уязвимости | Сведения подтверждены |
| Ссылки на источники | https://www.cybersecurity-help.cz/vdb/SB2021112905<br>http://thecyberthrone.in/2021/11/26/zeroday-vulnerability-in-tp-link-router/ |