Vulnerability Disclosure Plan for TP-Link Router

Objective

The objective of this vulnerability disclosure plan is to outline the steps and guidelines for responsibly reporting security vulnerabilities discovered in a TP-Link router as part of our ethical hacking course.

Scope

Target Device: TP-Link Router TL-MR3020
Method: Offline Local Testing
Compliance: Adherence to TP-Link's Responsible Reporting Guidelines and local laws

Steps for Vulnerability Disclosure

1. Vulnerability Discovery

Testing Environment: Ensure that all testing is conducted in a controlled environment to avoid any unintended disruptions or data breaches.
Firmware Version: Test the router using ddifferent firmwares. Among those the latest firmware to ensure the vulnerabilities are relevant and not already patched.

2. Documentation

Vulnerability Report: Document the vulnerabilities found in a clear and concise manner. Include the following details:

- Vulnerability Title
- Affected Product and Firmware Version
- Detailed Description of the Vulnerability
- Steps to Reproduce
- Potential Impact
- Recommended Mitigation

3. Reporting to TP-Link

We will use the dedicated communication channel provided by TP-Link for reporting vulnerabilities. We will submit the vulnerability report through the online form available on TP-Link's Security Advisory page.

4. Severity Assessment

We will assess the severity of the vulnerabilities based on industry standards (e.g., CVSS scoring).
We will prioritize the reporting of high-severity vulnerabilities to ensure timely action by TP-Link.

5. Follow-Up and Communication

Acknowledgment: Await acknowledgment from TP-Link regarding the receipt of the vulnerability report.
Cooperation: Maintain open communication with TP-Link throughout the disclosure process. Provide any additional information or clarification as requested.
Disclosure Date: Negotiate a disclosure date with TP-Link to ensure that the vulnerability is addressed before it is made public.

6. Public Disclosure (if necessary)

If TP-Link does not acknowledge or address the reported vulnerabilities within a reasonable timeframe, consider public disclosure to raise awareness such as Twitter to responsibly disclose the vulnerability, ensuring that the information is accurate and does not cause unnecessary panic.

Responsible Reporting Guidelines

All parties involved in the vulnerability disclosure process must comply with the laws of Denmark and th EU. Vulnerability reports should be based on the latest released firmware.
We will use the dedicated communication channel provided by TP-Link for reporting vulnerabilities. We will adhere to data protection principles and avoid violating the privacy and data security of TP-Link's users, employees, agents, services, or systems.
We will maintain communication and cooperation during the disclosure process and avoid disclosing information about the vulnerability prior to the negotiated disclosure date.
Note that TP-Link is not currently operating a vulnerability bounty program.