

Vulnerability Analysis and Exploitation of Legacy Firmware: A Case Study of Authentication Bypass in TP-Link TL-WR840N

Part 1: Executive Summary

1.1 Problem Statement

The subject device, a TP-Link TL-WR840N Wireless N Router, was in a state of administrative lockout due to forgotten credentials. Repeated failed login attempts triggered the device's internal security mechanism (Error 9003), enforcing a lockout period of over 4,000 seconds. The objective was to regain administrative access to retrieve critical Wide Area Network (WAN) Static IP configurations without performing a factory reset, which would result in the loss of ISP-specific configurations.

1.2 Chronology of Events

1. **Lockout:** Administrative access was denied; the device enforced a temporal lockout due to excessive failed attempts.
2. **Reconnaissance:** Initial scanning revealed the device was running a firmware version dated June 2018.
3. **Vulnerability Identification:** The firmware version was identified as vulnerable to **CVE-2018-12633**, an authentication bypass vulnerability involving HTTP Header manipulation.
4. **Exploitation:** By manipulating the Referer HTTP header, the authentication mechanism was bypassed. Initial attempts to query the internal API via JavaScript console injection failed due to non-standard internal object naming and the active lockout timer.
5. **Exfiltration:** After a physical power cycle to clear the lockout timer, the Referer header exploit was used to directly download the device's backup configuration file (Romfile.cfg).

6. **Decryption:** The binary configuration file was decrypted, revealing the plaintext admin password, WAN Static IP settings, and Wi-Fi credentials.

1.3 Vulnerability Profile

- **CVE ID:** CVE-2018-12633 (Authentication Bypass via Referer Header).
- **CVSS v3.x Score:** 9.8 (Critical).
- **Vector:** Network.
- **Complexity:** Low.
- **Privileges Required:** None.
- **User Interaction:** None.

1.4 Solution Overview

To remediate this vulnerability, the device firmware must be updated to a version released after late 2018. Additionally, the remote management feature must be disabled, and all compromised credentials (admin, Wi-Fi, PPPoE) must be rotated immediately.

Part 2: Technical Analysis and Exploitation

2.1 Understanding CVE-2018-12633

The vulnerability lies in the logic the router uses to validate requests. Instead of relying solely on a secure session cookie or token, the legacy web server (httpd) validates the **HTTP Referer Header**. If the request claims to originate from the router's internal main frame (http://192.168.0.1/mainFrame.htm), the server assumes the user has already authenticated and processes the request.

2.2 Exploitation: Step-by-Step Methodology

Phase A: Environment Setup

The attacker machine utilized:

- **Tool:** curl (Command Line Interface).
- **Tool:** Browser with "ModHeader" extension.

- **Target:** TP-Link TL-WR840N at 192.168.0.1.

Phase B: Bypassing the Lockout

The device responded with Error 9003 (Session Locked) to all requests. A physical power cycle was required to clear the volatile memory storing the lockout timer.

Phase C: The False Lead (JavaScript Injection)

Initial attempts utilized the browser console to query the router's internal API (\$.act functions).

- **Attempt:** \$.act(1, "WAN_IP_CONN", ...)
- **Result:** Error 71111.
- **Analysis:** The API endpoints were obfuscated or non-standard in this specific firmware version, rendering standard script-based injection ineffective.

Phase D: Data Exfiltration (The Successful Attack)

Instead of querying the API, the attack vector shifted to direct file retrieval using the Referer bypass.

Command Executed:

```
codeBash
```

```
curl -H "Referer: http://192.168.0.1/mainFrame.htm"  
"http://192.168.0.1/userRpm/Romfile.cfg" -o router_backup.bin
```

Outcome:

The command successfully downloaded router_backup.bin (Size: ~6KB).

Phase E: Decryption

The downloaded binary was encrypted using DES (Data Encryption Standard), common in TP-Link devices.

- **Tool Used:** RouterPassView / Custom Python Script.
- **Extracted Data:**
 - **User:** admin

- **Password:** yKuib45
- **WAN IP:** 192.168.1.33 (Static)

2.3 References

- *NIST National Vulnerability Database - CVE-2018-12633*
 - *TP-Link Security Advisory for Authentication Bypass*
 - *Exploit-DB: TP-Link WR840N Remote Configuration Disclosure*
-

Part 3: Defense and Mitigation Strategy

3.1 Immediate Remediation (Step-by-Step)

1. Firmware Upgrade (Critical):

- Navigate to **System Tools > Firmware Upgrade**.
- The current build (180614) is vulnerable. Install the latest available version from the vendor website. This patches the Referer header logic flaw.
- *Note: This effectively closes the door used in Part 2.*

2. Disable Remote Management:

- The extracted config revealed `<HttpRemoteEnabled val=1 />` on port 8080.
- Navigate to **Security > Remote Management**.
- Set the IP to 0.0.0.0 or select **Disable**. This prevents attackers from executing this exploit over the WAN/Internet.

3.2 Post-Exploitation Maintenance

Since the configuration file was decrypted, **all** secrets within it are considered compromised.

1. Credential Rotation:

- Change the Router Login Password immediately.

- Change the Wi-Fi (SSID) Passwords for both 2.4GHz and 5GHz bands.
- If PPPoE was used, contact the ISP to reset the broadband password.

2. Service Hardening:

- **Disable UPnP:** Prevents internal malware from punching holes in the firewall.
- **Disable WPS:** Mitigates PIN brute-force attacks (e.g., Reaver attack).

3. Network Segmentation:

- If the router cannot be updated (End of Life), place it behind a secure firewall or replace the hardware entirely.

Part 4: Recommendations and Future Outlook

4.1 Emerging Vulnerability Trends (Future Concerns)

While CVE-2018-12633 is a logic flaw, future vulnerabilities in embedded devices are trending toward more complex vectors:

- **SQL Injection in Embedded Web Servers:** As seen in **CVE-2025-29649** (SQLi in TP-Link login fields), vendors are increasingly using lightweight databases (SQLite) for session management, introducing SQLi risks previously rare in routers.
- **Command Injection in Diagnostic Tools:** Functions like "Ping" or "Traceroute" in the admin panel often lack input sanitization, allowing attackers to append shell commands (e.g., `; rm -rf /`).
- **Buffer Overflows in UPnP stacks:** Automated parsing of UPnP packets remains a high-risk area for remote code execution (RCE).

4.2 Thesis Summary

This study demonstrated that legacy hardware with outdated firmware presents a critical security risk. By exploiting **CVE-2018-12633**, we successfully bypassed authentication mechanisms that relied on client-side trust (HTTP Headers) rather than server-side verification.

The successful recovery of the router's configuration file underscores the importance of **Encryption at Rest**; had the configuration backup been encrypted with a unique, device-specific key (salt) rather than a hardcoded vendor key, the exfiltrated data would have been useless.

Final Recommendation: Hardware lifecycle management is paramount. Network infrastructure devices should be audited quarterly for firmware updates, and devices that no longer receive security patches should be decommissioned to prevent unauthorized network pivoting