Security Report: Vulnerabilities in Victure RX1800 WiFi 6 Router

Edward Warren

1 Introduction

This report details multiple critical security vulnerabilities discovered in the Victure RX1800 WiFi 6 Router (Model RX1800, Software Version: EN_V1.0.0_r12_110933, Hardware Version: V1.0). These vulnerabilities expose users to risks, including unauthorized access, arbitrary command execution with root-level permissions, and compromise of network integrity and confidentiality. Notably, the inability to disable certain services via the graphical user interface (GUI) necessitates command-line interface (CLI) interventions, which may be beyond the capabilities of the average user.

2 Summary of Vulnerabilities

2.1 1. Unauthenticated Telnet Root Access (CVE-2024-53938)

- **Description**: The Telnet service is enabled by default and exposed over the LAN. Critically, the root account is accessible without a password, allowing attackers to achieve full control over the router remotely without any authentication. There is no option in the router's GUI to disable the Telnet service; disabling it requires access to the CLI, which demands technical expertise.
- **Vulnerability Type**: Incorrect Access Control
- **Affected Component**: Telnet service exposed over LAN; root access without a password
- **Attack Type**: Remote
- **Impact**:
  - **Code Execution**: True
  - **Denial of Service**: True
  - **Escalation of Privileges**: True

  - **Information Disclosure**: True

- **Attack Vectors**: Unauthenticated attackers can access the device remotely without a password using the root account via the exposed Telnet service.

2.2 2. Default Admin Credentials Exposed Over LAN (CVE-2024-53937)

- **Description**: The Telnet service is enabled by default with `admin/admin` as default credentials and is exposed over the LAN. The device setup does not require this password to be changed during setup to utilize the device. The Telnet password is dictated by the current GUI password. Notably, there is no way to disable the Telnet service from the GUI; it must be done over the CLI.

- **Vulnerability Type**: Incorrect Access Control

- **Affected Component**: Telnet service with default `admin/admin` credentials exposed over LAN

- **Attack Type**: Remote

- **Impact**:

  - **Code Execution**: True
  - **Denial of Service**: True
  - **Escalation of Privileges**: True
  - **Information Disclosure**: True

- **Attack Vectors**: Attackers can gain root privileges via the exposed Telnet service enabled by default using default credentials.

2.3 3. Command Injection on Multiple Endpoints (CVE-2024-53939, CVE-2024-53940)

- **Description**: The router is vulnerable to (blind) command injection affecting multiple endpoints, including:

  - `/cgi-bin/luci/admin/opsw/Dual_freq_un_apple`
  - `/cgi-bin/luci/admin/opsw/ddns_apply`
  - `/cgi-bin/luci/admin/opsw/set_forward_cfg`
  - `/cgi-bin/luci/admin/opsw/ping_tracert_apply`
  - `/cgi-bin/luci/admin/opsw/set_pptp_l2tp_data_cfg`

These command injection vulnerabilities **require the attacker to be authenticated**. Remote attackers with valid credentials can exploit these vulnerabilities by sending crafted payloads to impacted parameters, executing arbitrary commands with root-level permissions. The absence of proper input validation allows attackers to inject malicious commands.

- **Vulnerability Type**: CWE-78: Improper Neutralization of Special Elements used in an OS Command (*OS Command Injection*)
- **Affected Components**: Multiple endpoints vulnerable to command injection
- **Attack Type**: Remote
- **Impact**:
  - **Code Execution**: True
  - **Denial of Service**: True
  - **Escalation of Privileges**: True
  - **Information Disclosure**: True
- **Attack Vectors**: Authenticated attackers can inject malicious commands via vulnerable parameters in the affected endpoints, leading to arbitrary command execution.

2.4 4. Weak Default Pre-Shared Key (PSK) Generation (CVE-2024-53941)

- **Description**: A remote attacker in proximity to a Wi-Fi network can derive the default Wi-Fi PSK value via the last four octets of the BSSID (in lowercase). The default PSK is generated based on these octets, making it predictable and vulnerable to unauthorized access.
- **Vulnerability Type**: Incorrect Access Control
- **Affected Component**: Default PSK generation based on last four octets of BSSID
- **Attack Type**: Remote
- **Impact**:
  - **Denial of Service**: True
  - **Escalation of Privileges**: True
  - **Information Disclosure**: True
- **Attack Vectors**: By observing the BSSID, an attacker can calculate the default PSK and gain unauthorized access to the Wi-Fi network.

3 Recommendations

3.1 For Users

1. **Change Default Credentials Immediately**: Upon setup, change both the GUI and Telnet passwords to strong, unique passwords.
2. **Disable Telnet Service via CLI**: Although not available via GUI, users with technical expertise should disable the Telnet service using CLI commands:

   ```
   service telnet stop
   chkconfig telnet off
   ```

3. **Configure a Strong Wi-Fi PSK**: Manually set a strong, random Wi-Fi password that does not rely on the default generation method.
4. **Discontinue Use** : There are no known firmware updates that address these vulnerabilities and the device appears abandoned by the manufacturer.

4 References

- https://www.newegg.com/p/2W6-002R-00004
- https://github.com/actuator/cve/tree/main/Victure

5 Conclusion

The vulnerabilities identified in the Victure RX1800 WiFi 6 Router pose serious security threats to users. The inability to disable the Telnet service via the GUI significantly hinders users ability to secure their devices. Immediate actions are required from both users and the vendor to mitigate these risks. Users should change default passwords and disable unnecessary services via CLI. The vendor should address these vulnerabilities promptly through firmware updates and enhanced security measures to protect users from potential exploits.