Teltonika RUT9XX Credential Brute force attack

Vulnerability Overview

Teltonika RUT9XX routers with firmware R_31.04.89 are prone to brute force vulnerabilities in /cgi-bin/luci.

- **Identifier** : Triad Cyber Security-ADV-20190217-01
- **Type of Vulnerability** : Brute force bypassing Ip blocking restriction
- **Software/Product Name** : Teltonika RUT950
- **Vendor** : Teltonika
- **Affected Versions** : Firmware RUT9XX_ R_31.04.89.
- **Fixed in Version** : RUT9XX_R_00.05.00.5 https://wiki.teltonika.lt/wiki/images/3/30/RUT9XX_R_00.05.00.5_WEBUI.bin
- **CVE ID** : CVE-2018-19879
- **CVSSv3 Vector** : CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L/E:H/RL:O/RC:C
- **CVSSv3 Base Score** : 7.1 (High)

Vendor Description

RUT950 is a professional industrial 4G LTE Wi-Fi router for IoT applications.
Source: https://teltonika.lt/product/rut950/

Impact

By exploiting the documented vulnerability, an anonymous attacker might have the capability to target a user and crack his password by using brute force tool.

It is recommend upgrading to version RUT9XX_R_00.05.00.5 or newer, which includes fixes for the vulnerabilities described in this advisory.

Vulnerability Description

The authentication functionality is not protected from automated tools used to make login attempts to the application. Anonymous attacker has the ability to make unlimited login attempts with an automated tool. This ability could lead to cracking a targeted user's password.

By cracking the password, the attacker might take over the router administration panel allowing full access to:

- ✓ Changing the router settings including: change of traffic routing settings thus damaging data integrity.
- ✓ Adding static DNS records diverting traffic to a different IP thus damaging the availability and integrity of the data.
- ✓ Backing up the configuration discovering its wireless network passwords thus damaging the confidentiality of the data

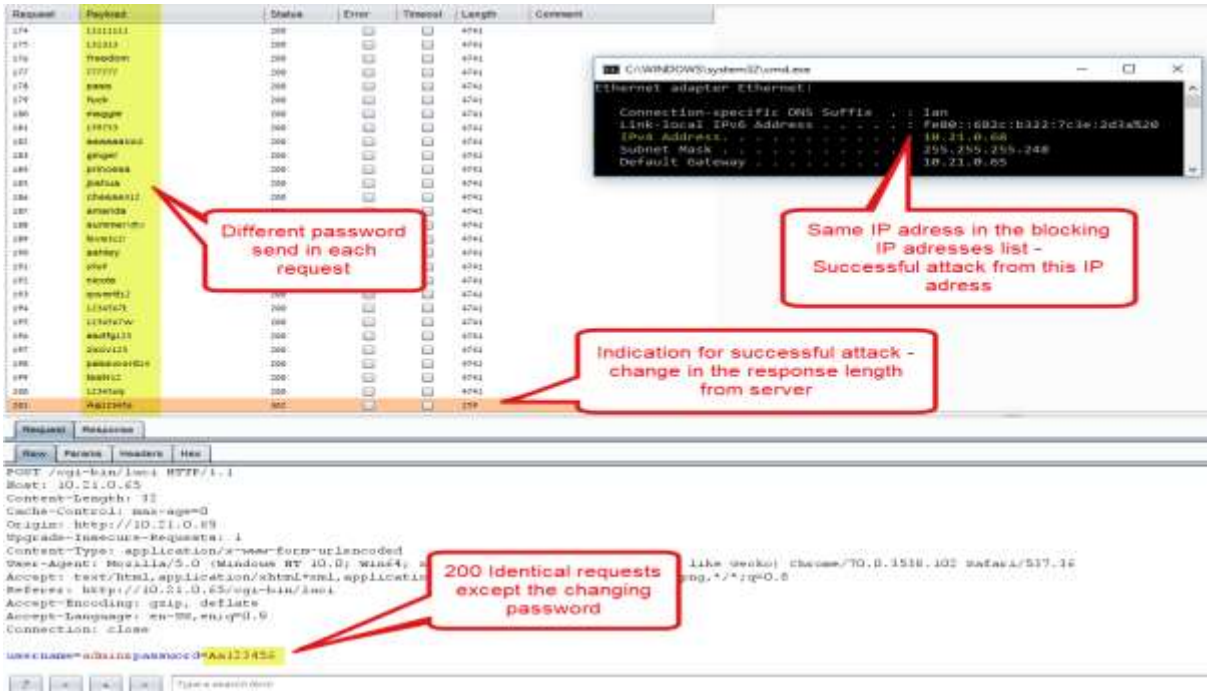
More concretely, the following parameters are vulnerable:

- /cgi-bin/luci

Proof-of-Concept

The following screen capture demonstrates an attacker's blocked IP address in the router management interface:

The following screen capture demonstrates a Brute-Force attack on the authentication interface to retrieve a password of an existing user with the same IP address that is "blocked" in the router management interface:



Timeline

- 18-11-2018 identification of vulnerability in version RUT950_R_31.04.89
- 26-11-2018 initial vendor contact through public address
- 29-11-2018 vendor response with security contact
- 29-11-2018 disclosed vulnerability to vendor security contact
- 05-12-2018 vendor test the vulnerability and confirm.
- 05-02-2019 verification that the vulnerability has been fixed in version RUT9XX_R_00.05.00.5.

References

- Firmware Changelog: https://wiki.teltonika.lt/index.php?title=RUT9xx_Firmware

Credits

- Tal Argoni (Triad Security Research)
- Matan Frank (Triad Security Research)