USR IOT 4G LTE Industrial Cellular VPN Router 1.0.36 Remote Root Backdoor

Title: USR IOT 4G LTE Industrial Cellular VPN Router 1.0.36 Remote Root Backdoor
Advisory ID: ZSL-2022-5705
Type: Local/Remote
Impact: Exposure of Sensitive Information, Security Bypass, System Access, DoS
Risk: (5/5)
Release Date: 20.04.2022

Summary

USR-G806 is a industrial 4G wireless LTE router which provides a solution for users to connect own device to 4G network via WiFi interface or Ethernet interface. USR-G806 adopts high performance embedded CPU which can support 580MHz working frequency and can be widely used in Smart Grid, Smart Home, public bus and Vending machine for data transmission at high speed. USR-G806 supports various functions such as APN card, VPN, WIFIDOG, flow control and has many advantages including high reliability, simple operation, reasonable price. USR-G806 supports WAN interface, LAN interface, WLAN interface, 4G interface. USR-G806 provides various networking mode to help user establish own network.

Description

The USR IOT industrial router is vulnerable to hard-coded credentials within its Linux distribution image. These sets of credentials are never exposed to the end-user and cannot be changed through any normal operation of the device. The 'usr' account with password 'www.usr.cn' has the highest privileges on the device. The password is also the default WLAN password.

Vendor

Jinan USR IOT Technology Limited - https://www.pusr.com

Affected Version

1.0.36 (USR-G800V2, USR-G806, USR-G807, USR-G808)
1.2.7 (USR-LG220-L)

Tested On

GNU/Linux 3.10.14 (mips)
OpenWrt/Linaro GCC 4.8-2014.04
Ralink SoC MT7628 PCIe RC mode
BusyBox v1.22.1
uhttpd
Lua

Vendor Status

[10.04.2022] Vulnerability discovered.
[14.04.2022] Vendor contacted.
[19.04.2022] No response from the vendor.
[20.04.2022] Public security advisory released.

PoC

usriot_root.py

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://packetstormsecurity.com/files/166813/
[2] https://cxsecurity.com/issue/WLB-2022040086
[3] https://exchange.xforce.ibmcloud.com/vulnerabilities/224930
[4] https://www.exploit-db.com/exploits/50894
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29730
[6] https://nvd.nist.gov/vuln/detail/CVE-2022-29730

Changelog

[20.04.2022] - Initial release
[03.05.2022] - Added reference [1], [2] and [3]
[13.05.2022] - Added reference [4]
[29.05.2022] - Added reference [5] and [6]

Contact

Zero Science Lab

Web: https://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Rete mirabilia**
- **We Suggest**
- **Profiles**
- Site Meter