NavigateWorx

NavigateWorx White Page for General Router Security

www.navigateworx.com

Overview

With mass deployment of router devices, both Consumer-grade and industrial-grade routers are facing similar security risks, which mainly comes from simple operation of routers and the homogeneity of functions. The operation of modern routers is generally configured through web login. Compared with the operation mode of enterprise-level router deployment, Login and configure via web increase certain risks. For example, public Wi-Fi routers often mentioned have been maliciously implanted with Trojan horses, and users connected to public Wi-Fi have acts of fraud information or passwords on computers or mobile phones.

In the field of industrial-grade cellular network routers, more customers may be concerned about whether the SIM card fraud, someone use the SIM cards in illegal way will cause data traffic to exceed limitation and receive a large bill from the mobile operators. In fact, the operational risk of industrial-grade cellular network routers is not only caused by the SIM card tariffs, which leads to financial losses, because industrial-grade cellular network routers are widely used in various applications and the number of deployments is very large, from smart grid power supply equipment to bank financial machines, self-service vending machines, smart city traffic monitoring devices, video surveillance devices, etc., Once a router is maliciously damaged due to project problems and operational risks, the loss caused is far bigger than the financial part. Therefore, improving the risk awareness of industrial-grade routers currently should to be a very urgent part!

Part 1 - SIM Card Security

The SIM card is one of the most important part of wireless cellular routers accessing to the internet. Among many questions raised from customers / integrators, the main question is how to avoid the loss of data charges caused by the theft of the SIM card.

In fact, there are different types of SIM cards, such as normal SIM cards, specific SIM cards for M2M applications, and SIM cards that can obtain public IP addresses. Of course, with the development of mobile technology, there are some special SIM cards presented in the market. eSIM (electronic chip) or vSIM (no physical SIM chipset) has been applied in some countries, but the traditional SIM card applications are still very popular, so the first step of SIM card security, is to distinguish the types of SIM cards.

1. If you are using a normal SIM card, the SIM card will obtain private IP generally, which will not cause security problems of being accessed from the Internet. However, if the SIM card is stolen, the SIM card data is probably to be used by others.

   Suggestion: Add PIN verification on SIM card.

2. If you will deploy a lot of routers for one project, you can apply for special M2M SIM cards from local mobile operators. Those SIM card would only allow access to the network when the designated SIM card APN is configured; or after the router is replaced, the SIM card will become invalid, which can avoid the SIM cards be stolen.

   Suggestion: Apply for specific SIM cards for M2M applications with operators.

3. If you need use a SIM card with a public IP address, please pay attention to the device configuration to enable multiple protection measures, such as disable ICMP reply / HTTP / HTTPS / SSH / Telnet, and add a specific port to access the device, add filter settings in the firewall.

   Suggestion: Try not to use a SIM card with public IP address, or follow above suggestion to reduce the risk be hacked.

Part 2 - Physical Interface Security

As a general function of router, plug and play on the Ethernet port should be enabled by default. When a computer is plugged to a router (or connected via Wi-Fi), it should be able to access the Internet. However, when industrial IoT applications are deployed in projects, it will possibly become a "back door" of router security. For example, non-engineers connect terminal devices randomly to the router, this will cause operation risks and waste SIM card data traffic.

Suggestion:

1. Disable DHCP. At the end of project, we are clear that which devices will be connected to the router by Ethernet ports or wireless. It is recommended to turn off the DHCP function and let the engineer mark the static IP address of the terminal devices. This can reduce the number of unknown devices connecting to routers to surf the Internet.
2. If you need to enable DHCP, configure the MAC address binding of regular used devices, and only designated devices can obtain IP through DHCP.
3. Change the default IP address of the router's LAN port so that it is not in the same network segment as the default IP address marked on the label.

Part 3 - Wi-Fi Security

Most routers on the market now support Wi-Fi AP mode, which allows customers to access the Internet via Wi-Fi. In recent years, the deployment of industrial IoT application with Wi-Fi has gradually increased. In these scenarios where wiring is very difficult, Wi-Fi, as a mature technology, is indeed a good choice.

Nowadays Wi-Fi is very common, this section will focus on improving Wi-Fi security settings on router.

Suggestion:

1. Do not use the unencrypted mode to provide Wi-Fi access, but should adopt higher security standards, such as WPA/WPA2 encryption mode.
2. If Wi-Fi AP broadcast is only provided to a few terminal devices, the SSID broadcast mode can be disabled, which can reduce the risk of being attacked.
3. In addition, you can also cooperate with the Radius server to check the verification of Wi-Fi client access.

Part 4 - Device Login Security

The security of device login is to prevent unauthorized engineers from modifying the running configuration, because the device not operate normally will cause unpredictable risks to the project. For production reasons, almost all manufacturers prompt the default IP address and username/password for router login on the label.

Suggestion:

1. Modify router's default login user name and password.
2. If condition allows, you can also cooperate with the Radius server to verify the security of user login.
3. If the project requires different authorized engineers to configure or observe the operating status of the routers, you can use our different authorizations for users, such as administrators and read-only users.
4. When accessing the device from the outside, it is recommended to use HTTPS instead of HTTP, because HTTP is transmitted in plain text on the network, and the content of the configuration can still be known through packet capture.

Part 5 - VPN Options

Refer to the above suggestions, the safety of the cellular router has been improved. However, for some important and very sensitive data, it is not enough yet.

Regarding to security of data transmission, the most widely used technology is VPN (Virtual Private Network). The data transmission on the public network is ensured by encrypting the data before it reaches the destination and decrypting it by the peer device.

Navigateworx Router already support multiple VPN, such as OpenVPN, PPTP, L2TP and IPSEC, DMVPN.

Part 6 - NavigateWorx Security

In the software and hardware design of Navigateworx's router, safety performance is also considered very seriously.

For example, our router has the following security policies:

1. Navigateworx develop own OS to ensure software security, it is much safe than an open source system on the Internet.
2. The password input method has been encrypted and protected, for example, the page only displays **** instead of the password string.

MORE INFO

Please visit **www.navigateworx.com**

Contact us **sales@navigateworx.com**

Suggestion:

1. If the terminal device connected behind the router has Ethernet port and supports VPN technology, then it can directly establish VPN with the VPN server to ensure data encrypted transmission. Of course, you can use the VPN supported by the router itself as well, it will establish VPN with remote VPN server to ensure safe data transmission.
2. If the terminal device connected behind the router only supports serial port, then VPN tunnel needs to be established between the router and the VPN server. The serial port of our router only needs to be configured as a TCP server or a TCP client. After the data of terminal serial device reaches our router, it can also be encrypted and transmitted to the remote data center through the VPN channel, ensuring the security and integrity of the data.
3. Firmware is encrypted and the exported device operating status Diagnostic file is encrypted.
4. Router supports general firewall, which can filter unnecessary external access requests and filter unreasonable internal requests by keywords
5. Navigateworx router is connected to the own Device Management Platform by verifying the x.509 certificate.