Security Guidelines

APPLICATION NOTE

ADVANTECH

Used symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that can arise in specific situations.

Information, notice – Useful tips or information of special interest.

Example – Example of function, command or script.

Vulnerability Reporting

For security inquiries and for submitting a vulnerability report please contact your customer support.

Customer Support for NAM

E-mail: support@advantech-bb.com
Web: www.advantech-bb.com

Customer Support for Europe

E-mail: iiotcustomerservice@advantech.eu
Web: www.advantech-bb.com

Customer Support for Asia

E-mail: icg.support@advantech.com.tw
Web: www.advantech.com

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic.
Document No. APP-0078-EN, revision from May 6, 2020. Released in the Czech Republic.

Contents

Introduction

This document describes guidelines for securing the router and keeping it secure during installation, configuration, operation, maintenance and decommissioning. It includes best practices and tools recommendations.

The document however, does not cover system-level security. It does not describe how to build and maintain secure networks. It does focussolely on securing the router.

The document contains two main parts:

1. **Hardening Guide** with focus on installation and configuration, including:
    - Architectual considerations for integration into intended environment
    - Security measures expected to be provided by the external environment
    - Configuration options providing the highest security
2. Recommendations for **Secure Operation** with focus on monitoring, maintenance and decommissioning, including:
    - Account permissions (roles) needed to operate the router
    - Responsibilities and actions for network administrators
    - Operational policies and procedures

Security features

Advantech cellular routers offer the following security capabilities:

- **Firewall and NAT** filter incoming and outgoing network traffic based on a set of rules.
- **WiFi authentication and encryption** prevents unauthorized clients from connecting and protects the wireless network communication.
- **VPN (either OpenVPN or IPsec)** protects integrity and confidentiality of network communication between two routers.
- **Connection to a central Syslog server** enables remote monitoring of significant events on the router such as reboots, user logins or configuration changes.
- **Automatic Update** ensures the router is running the latest firmware with all available security patches.

1. Hardening Guide

The following sections provide hardening guidelines for cellular routers manufactured by Advantech Czech. Whereas the *Configuration Manual* describes all capabilities and configuration options of your router, this Hardening Guide provides a checklist to verify the configuration is optimized for highest security.

Each section describes:

- **Weakness** which may arise from a misconfiguration;
- **Defaults** factory settings; (This may differ if you are using a customized configuration module.)
- **Hardening** guidelines to mitigate the weakness. These assume firmware version 6.2.4 or above.

The router configuration is initially set to defaults of the factory firmware version. It can be reset to defaults of the currently installed firmware version by pushing/holding the *RST* button.

The configuation is not modified during firmware upgrade. For example, if you used 6.1.7 with its default settings, you will still use these settings after upgrading to 6.2.4.

1.1 No Physical Access

Weakness

Malicious persons that have physical access to the device can easily disrupt its operation. An attacker may destroy or disconnect the device, extract credentials from its memory, modify the device or replace it with a malicious device under the control of the attacker.

Defaults

Cellular routers are protected against industrial environmental conditions (see the corresponding Data Sheet for more details).

Hardening

1. Create a secure environment, which can be accessed by authorized personnel only.
2. Protect power supply from (un)intentional disconnection. For critical systems use Uninterruptible Power Supplies (UPSs).
3. Protect input and output cabling.

1.2 Disable non-root login

Weakness

The router security features protect from external threats, assuming there are no local non-root users that could log-in and perform malicious actions. For example, there are no user resource quotas, so non-root users that can log-in could execute a CPU/memory intensive software and disrupt router functions.

Defaults

The router supports two *Roles*:

- **Admin**, who has full access rights to setup and configure the router and a remote shell access;
- **User**, who can only view the router status from the web administration and access the user data storage via (S)FTP. No other remote access.

Users created via the web interface have their login shell set to */bin/false*, so they cannot login.

Hardening

Never make manual changes to the */etc/passwd*. Never allow non-root users command line access to the router.

1.3 Enable Wi-Fi security

Weakness

Wi-Fi Authentication prevents unathorized persons from connecting to the network. When disabled, anonymous attackers may spread viruses, perform Denial of Service (DoS) attacks on the network or connected clients or just steal the bandwidth.

WI-Fi Encryption protects the communication from eavesdropping by other persons. When disabled, attackers may intercept your login credentials or other sensitive data.

Defaults

The following *Authentication–Encryption* combinations are allowed:

- **Open–None** doesn't use any authentication nor encryption. This is the default, but least secure option.
- **Open–WEP** uses the WEP key for encryption only. The WEP cipher is not secure as it can be broken in few minutes.
- **Shared–WEP** uses WEP key both for authentication and encryption. This is even less secure than Open - WEP as the authentication phase allows easier data interception.
- **802.1X–WEP** uses RADIUS to authenticate and then derives the WEP key for encryption. As stated above, the WEP encryption is not secure.
- **WPA–TKIP** uses the original WPA protocol. It is not secure; use WPA2 instead.
- **WPA–AES** uses WPA with a more secure EAS instead of TKIP. This is intended for rare devices that support AES, but don't support WPA2.
- **WPA2–TKIP** uses the modern WPA2 with older TKIP. Use only if you have older devices that cannot use WPA2–AES.
- **WPA2–AES** uses the standard WPA2. This is the most secure option.

The WPA and WPA2 can either use a Pre-Shared Key (PSK) or a RADIUS (Enterprise) authentication.

Hardening

Always enable **WPA2–AES** to protect security of the user communication. When a weaker authentication needs to be used for compatibility reasons, consider using *Accept List* to explicitly identify clients that are allowed to connect.

When a weaker encryption needs to be used, consider using a VPN (OpenVPN or IPsec) to protect the transmitted information.

1.4 Enable Wi-Fi isolation

Weakness

In a public Wi-Fi network the Pre-Shared Keys (PSK) are often well known, so the operator cannot effectively prevent malicious users from connecting to the wireless network. When the connected users are not isolated enough, such malicious users could then use the network to attack other connected users.

Defaults

By default, both *Bridged mode* and *Client Isolation* is disabled.

Hardening

To further protect security of the connected devices:

1. Make sure the *Bridged mode* is disabled.
2. Enable *Client Isolation*.
3. Configure *Firewall* to prevent device to device communication: *Enable filtering of forwarded packets* and then for example (in this order):
   - **allow** all protocols with *Source* in the IP range of WiFi devices
   - **deny** all protocols with *Destination* in the IP range of WiFi devices

   This will prevent inter-user traffic on the WiFi network and also prevent external sources from initiating sessions with the WiFi clients.

1.5 Disable unused services

Weakness

Enabled services provide additional attack surface for attackers to exploit. They can use flaws in the enabled network services, their protocols or configuration to compromise the device or perform Denial of Service attacks.

Defaults

Most services are disabled by default. Only the following ones are enabled:

- DHCP on primary LAN (eth0)
- HTTPS
- SSH
- SNMP

In addition to that, the following services were enabled on v3 platforms until v6.1.0 and on v2 platforms until v6.2.0:

- HTTP
- FTP
- Telnet

Hardening

1. Remove user modules that are not necessary.
2. Disable services, ports and protocols that are not necessary.

   Consider disabling services like SSH that are used only occasionally for manual maintenance. Such services can be enabled only when maintenance is needed and disabled afterwards.

Always keep enabled one service for remote management, i.e. either the HTTPS (for web-admin) or Hosted Management (HMP) Client (for WebAccess/DMP).

1.6 Use restrictive firewall

Weakness

Firewall prevents unauthorized access to/from the LAN. Its misconfiguration may impact confidentiality, integrity or availability of your network and/or devices.

Defaults

The router distinguishes outer (WAN) and inner (LAN) side. Initially, the firewall only drops traffic to well-known services[1] coming from WAN and allows all communication coming from LAN.

Hardening

1. The *Firewall* shall allow only as little incoming traffic as necessary.
2. *Enable filtering of incoming packets* and define IP addresses or IP ranges (e.g. *10.0.0.0/8*) of systems deployed in the WAN that need to send packets to the router such as your central management server (if any). Packets sent by non-matching addresses will be denied by default. **These settings do not apply to LAN interfaces.**
3. *Enable filtering of forwarded packets* and define IP addresses or IP ranges from both WAN and LAN that can send packets forwarded (routed) by the router. Other packets will be dropped.
4. *Enable filtering of locally destinated packets* to drop all packets sent to the router's IP address, except packets sent to the enabled services (Telnet, FTP, etc.)
5. *Enable protection against DoS attacks*. This will protect you against the most common attacks:
   - TCP SYN flooding (allows max 3/sec)
   - ICMP Echo flooding (allows max 3/sec)
   - DoS using small MSS (allows min 250)
6. The *NAT Configuration* shall enable port forwarding and *remote access* only to the services that are used. Disable what is not needed.

Related to CVE-2010-4563, CVE-2019-11479, Nessus-50686.

[1] FTP, SSH, Telnet, DNS, HTTP(S), SNMP

1.7 Disable FTP

Weakness

The File Transfer Protocol (FTP) provides a basic, unencrypted file transfer capability with cleartext passwords for authentication. Attackers can easily eavesdrop user passwords or use man-in-the-middle attacks to maliciously alter the transferred data or inject malware.

Defaults

The FTP is configurable since v6.1.0. Since the firmware v6.2.0 the the FTP service is disabled by default.

Before v6.2.0 the FTP was disabled on v3 routers. On v2 routers it was enabled, but accessible from LAN only. The remote access from WAN has always been denied.

Hardening

1. The FTP service shall be disabled. For a secure file transfer the SSH-based SFTP should be used instead.

   FTP may only be used with extreme legacy systems in isolated networks that are periodically scanned for malicious software.

2. When enabled, limit *Maximum Sessions* and *Session Timeout*.

3. The *remote FTP access* in the *NAT* configuration shall be disabled in any case. Never use FTP in public Internet.

1.8 Disable Telnet

Weakness

Telnet provides a simple terminal session to the router. The Telnet protocol provides no built-in security measures. Attackers can easily eavesdrop the entire communication, including the root password.

Defaults

The Telnet is configurable since v6.1.0. Since the firmware v6.2.0 the the Telnet service is disabled by default.

Before v6.2.0 the Telnet was disabled on v3 routers. On v2 routers it was enabled, but accessible from LAN only. The remote remote access from WAN has always been denied.

Hardening

1. The Telnet service shall be disabled. For a secure terminal session the SSH service should be used instead.

   Telnet may only be used with extreme legacy systems in isolated networks that are periodically scanned for malicious software.

2. When enabled, limit *Maximum Sessions*.

3. The *remote Telnet access* in the *NAT* configuration shall be disabled. Never use Telnet in public Internet.

Related to Nessus-42263.

1.9 Disable (unencrypted) HTTP

Weakness

The router administration using HTTP uses unencrypted communication. Attackers thus can easily eavesdrop the user credentials.

Defaults

Since v6.1.0 the following configuration options are possible:

Enable HTTP	Enable HTTPS	HTTP Access	HTTPS Access	Router behaviour
Off	Off	Off	Off	Web server completely down
Off	On	Redirect	On	Forced redirect HTTP to HTTPS
On	Off	On	Off	HTTP access only
On	On	On	On	Independent HTTP or HTTPS access

The HTTPS is available and always enabled on v2 and v3 router platforms. Since the firmware v6.2.0 the HTTP is disabled by default.

Before v6.2.0 the HTTP was disabled on v3 routers. On v2 routers it was enabled, but accessible from LAN only. The remote access from WAN has always been denied.

Hardening

1. Disable the HTTP service and enable HTTPS instead.
2. Both *remote HTTP access* and *remote HTTPS access* shall be disabled. The web administration shall not be accessible from the Internet.

Related to Nessus-26194.

1.10 Use secure HTTPS ciphers

Weakness

The HTTPS protocol is based on a secure transport layer that comes in multiple versions. Some of the transport layer versions are no longer considered sufficiently secure and should not be used:

- SSL 2.0 is prohibited by RFC 6176 since 2011.
- SSL 3.0 is prohibited by RFC 7568 since 2015.
- Also TLS 1.0 and TLS 1.1 will too be soon deprecated by a future RFC.

Defaults

The SSL 2.0 has never been enabled. The SSL 3.0 is permanently disabled since v5.0.0. The TLS 1.0 and TLS 1.1 are however enabled for compatibility reasons.

Hardening

Set *TLS/SSL Min Protocol Version* to **TLS 1.2**.

1.11 Use a proper HTTPS certificate

Weakness

Certificate proves a router identity to the Web broswer. If the certificate cannot be trusted, then there is a risk that the browser is connected to fake server. The attacker may trick the user to connect to a fake server and obtain the root password.

Defaults

During initialization the router generates a self-signed certificatie, which cannot be trusted.

Hardening

Obtain a HTTPS certificate from a public or your corporate Certification Authority (CA). Then *Upload a new certificate* to your *HTTP Configuration*. The HTTPS certificate shall be:

- Within its validity time period;
- Signed by a trusted certificate authority, i.e. not self-signed.

Check of the validity period requires a correct time. To ensure the certificate will remain valid even when the RTC battery or NTP server communication fails the certificate validity period should start on 1.1.1980.

You can verify validity of your certificate by clicking on the Lock Icon in your Web browser.

Related to Nessus-51192, Nessus-57582.

1.12 Use secure IPsec ciphers

Weakness

The following algorithms are broken in regards to security:

- Encryption: DES, 3DES, CAST, BLOWFISH
- Hash: MD5, SHA-1
- DH Group: 2 and lower (MODP512, MODP768, MODP1024)

Authentication Mode using a Pre-Shared Key is less secure than using a X.509 certificate. A Pre-Shared Key is often cryptographically weaker and when leaked, an attacker can mount a man-in-the-middle attack to impersonate either side and intercept the traffic passing through the tunnel.

Defaults

By default *IKE Protocol* **IKEv1**, *IKE Mode* **main** and *IKE Algorithm* **auto** is used. This selects aes128-sha256-modp3072, which complies to the NIST mandate that a minimum cryptographic strength of 128 bit is sufficient for security beyond the year 2030.

The *ESP Algorithm* **auto** is used, which defaults to aes128-sha256.

Once you set the *auto* mode the default algorithms will be used. The individual algorithm configuration fields turn grey and the pre-filled values will be ignored.

Hardening

1. Do not use the broken algorithms listed above. Preferrably, stick to the default IKE and ESP settings.

   For the manual IKE use as a minimum the *IKE Encryption* **AES128**, the *IKE Hash* **SHA256** and the *IKE DH Group* **15** (MODP3072).

   For systems not supporting SHA-256, SHA-1 might be used instead. SHA-1 must not be used as anything else than a HMAC for IKE.

   For the manual ESP use as a minimum the *ESP Encryption* **AES128** and the *ESP Hash* **SHA256**.

2. The *IKE Mode* shall be **main**. It is strongly advised to avoid the aggressive mode as it is inherently flawed.

3. *Authenticate Mode* using **X.509 Certificate** is recommended. Certificates should be signed using at least SHA-256.

   To securely authenticate using a Pre-shared Key it has to be very long and random. A good way to generate such key is for example:

   ```
   dd if=/dev/urandom count=1 bs=32 2>/dev/null | base64
   ```

4. The *PFS* (Perfect Forward Secrecy) should be enabled for every tunnel. It protects the confidentiality of the traffic, if the IKE shared secret has leaked.

For more details please see the strongSwan documentation.

1.13 Use complex SNMP community

Weakness

The SNMP *Community* string is like a password that allows access to router configuration and statistics.

An attacker who is able to guess the *Read Community* string can retrieve sensitive network information for further attacks, or overwhelm the router with massive traffic and cause service interruption.

After activating *Enable I/O extension* the SNMP can be used to modify an I/O status. Attacker that is able to guess the *Write Community* string could maliciously control the connected system.

Defaults

The *SNMP agent* and *SNMPv1/v2 access* is by default enabled and accessible via LAN only. The agent uses **public** as a *Read Community* and **private** as a *Write Community* string. This is a common default for many devices.

The *I/O extension* is disabled by default.

Hardening

1. Disable the *SNMP agent* when not needed.
2. Disable *SNMPv1/v2 access* and *Enable SNMPv3 access* which employs better encryption.
3. Disable SNMP extensions that are not needed.
4. Configure *Firewall* to restrict the UDP traffic on port 161 (SNMP) to the monitoring servers only.
5. The *remote SNMP access* in the NAT configuration shall be disabled. Never use SNMPv1/v2 in public Internet.
6. Set the *Read* and *Write Community* strings to a non-trivial value that cannot be easily guessed.

Related to CVE-1999-0524, Nessus-41028 and Nessus-76474.

1.14 Mitigate Sockstress[2] attack

Weakness

A design flaw in the TCP protocol allows an attacker to create crafted TCP connections, which can eventually exhaust the router resources and lead to a denial of service (DoS).

Defaults

No TCP service is accessible from WAN, so the attack is possible from LAN only. Attackers in LAN may cause a Denial of Service (DoS) of any accessible TCP service, including SSH or HTTP(S) administration.

Hardening

The only way to completely prevent this attack is to whitelist access to TCP services in the *Firewall* configuration.

Note: The current firmware does not support rate limitation of TCP connections with iptables.

Related to CVE-2008-4609.

[2] https://en.wikipedia.org/wiki/Sockstress

2. Secure Operation

The following sections provide recommendations for a secure monitoring, maintenance and decommisioning of cellular routers manufactured by Advantech Czech.

Each section describes:

- **Risk** related to router operation;
- **Recommendation** to mitigate the risk. These assume a firmware 6.2.4 or above.

2.1 Use latest firmware

Risk

Due to the shipping and storage time even newly delivered routers may contain an older firmware.

The firmware is based on a large number of software components. We continuously fix the security vulnerabilities discovered in these components, so the older firmware versions may be affected by some of the publicly known vulnerabilities. An attacker may use this information to disrupt the router functions or steal sensitive information.

New firmware versions also may include new configuration options to improve the router security.

Recommendation

1. Subscribe for firmware update notifications. You can either subscribe to our RSS channel https://ep.advantech-bb.cz/blog/rss our (when registered to our Portal) to e-mail motifications for specific router models[1].

2. Upgrade your firmware as soon as possible.

   For a large number of routers it is recommended to establish a HTTP/FTP server in your infrastructure, store to some directory the *.bin* and *.ver* files of the latest firmware package, then *Enable automatic update of firmware* and point *Base URL* to that directory.

3. After upgrading, download the latest *Hardening Guide* and verify the security configuration.

[1] https://ep.advantech-bb.cz/support/router-models

2.2 Use complex passwords

Risk

The default username is **root**. The default password is:

- Unique auto-generated string, which is printed on the router's label.
- **root**, if the unique password is not used for your router.

If the password is weak the attacker may guess it, connect to the router and perform malicious actions. This is even worse if the same password is reused for multiple routers.

Recommendation

1. If multiple persons need to access the router, create muliple accounts, one for each person.
2. Use passwords that are complex enough, so either a word mixing letters, numbers and other characters, or (better) a sentence of multiple words.

   Mike Halsey created a chart[2] that shows how long it would take a modern computer to crack passwords of varying complexities.
3. Never use the same password for all your routers.

   If you have too many routers to manage (and thus too many passwords), consider using the WebAccess/DMP or some password manager, e.g. Bitwarden.
4. Keep the password secret; do not share it with anyone.

[2] https://www.ghacks.net/2012/04/07/how-secure-is-your-password

2.3 Use encrypted backups

Risk

Depending on check-box settings one can:

- *Backup configuration*, including PIN for Mobile WAN, Pre-Shared Keys (PSK) for Wi-Fi or private keys for OpenVPN/IPsec.
- *Backup users*, including all password hashes in */etc/shadow*.

When the backup is not encrypted an attacker could obtain the stored sensitive information and e.g. misuse the PIN, PSK or try to crack the root password.

By default, only configuration is stored.

Recommendation

A non-trivial *Encryption Password* should be used during any *Configuration Backup*. It must not be left blank.

2.4 Monitor system logs

Risk

When routers are deployed in the field attackers may attempt to login or otherwise maliciously interact with the router. If unattended, the attack attempt may not be detected so the attacker will have enough time for several attempts, which increases the likelihood of a success.

You can view the system messages on the *System Log* screen or *Save Log* to a file, but this is impractical when you have a high number of routers.

Recommendation

1. Setup a log collection and analysis server (e.g. Graylog) and let it listen for Syslog UDP messages.
2. In the *Syslog* service configuration enter the *Remote IP Address* of the log collection server.
3. Setup the server to automatically identify security relevant events such as:
   - Router reboots
   - Both successfull and failed login attempts
   - Changes to the router configuration
   - Clients connecting to the WiFi AP

2.5 Disable lost devices

Risk

Devices deployed in the field may be stolen or get lost. An attacker who possesses a cellular router may:

- Use the WAN connectivity paid by the device owner;
- Access the owner's network via the configured VPN;
- Retrieve confidential data (e.g. certificates) stored on the device.

Recommendation

1. Keep a record of active devices and associated digital assets, such as passwords, certificates, keys or SIM cards.
2. Detect loss of a device as quickly as possible. When lost, all associated assets shall be considered as compromised:
    - Deactivate SIM cards used in the device;
    - Disable all accounts that use any of the passwords that were stored in the device;
    - Revoke certificates for all private keys stored on the device.

2.6 Remove stored data when decommissioning

Risk

The router configuration contains sensitive data, such as certificates, passwords or PINs. It may also be used to collect and/or store sensitive information from other machines. When the router is sent for maintenance or disposal, the stored information may leak to unauthorized persons.

Factory Reset using the *RST* button deletes the custom configuration, but does not delete user certificates nor any other user data stored on the router.

Recommendation

1. Remove installed user modules. This will also remove user data related to these modules, except WA/VPN certificates.
2. Delete all remaining sensitive information in /var/data.
3. If you uploaded own HTTPS certificate, *Generate a new certificate* to overwrite your certificate with a generic, self-signed one.
4. Perform Factory Reset by pushing/holding the *RST* button (see the User Manual). Then, wait until the *PWR* LED starts blinking again.
5. Power off the device and remove all SIM cards.
6. Remove all references to the device from network servers like DHCP or DynDNS.