Security Guidelines

APPLICATION NOTE

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

We proactively search for security deficiencies in our products and continuously update Vulnerability Advisories. These are available through our Security inquiries and reports page.

If you have discovered a security vulnerability in cellular routers developed by Advantech Czech, please send a Report to security@advantech.cz.

For other product related questions please contact the Advantech technical support.

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic.
Document No. APP-0078-EN, revision from November 10, 2022. Released in the Czech Republic.

Contents

Introduction

This document describes guidelines for securing an Advantech cellular 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 focus solely on securing the router.

When some router apps are installed, additional hardening may be required.

This document contains three parts:

1. Description of **Security Features** provided by the cellular router in its default configuration;
2. Recommendations for **Secure Operation** with focus on monitoring, maintenance and decommissioning;
3. **Hardening Guide** with focus on installation and configuration.

The following subjects are covered in this document:

- Security measures expected to be provided by the external environment, see Section 1.3.
- Responsibilities and actions for network administrators, operational policies and procedures, see entire Chapter 2.
- Configuration options providing the highest security, see entire Chapter 3.
- Account permissions (roles) needed to operate the router, see Section 3.2.
- List of default network communications, port numbers and service types, see Section 3.5.

Detailed description of features and all individual configuration options of a specific router can be found in a respective *Configuration Manual* [EP].

1. Security Features

1.1 Network segmentation

As introduced in the *User Manual*, Advantech cellular routers are designed to provide:

- Access to the Internet from LAN;
- Backed up access to the Internet;
- Secure network interconnection using a Virtual Private Network (VPN);
- Connection of a Programmable Logic Controller (PLC) via a Serial Gateway.

In any of these four situations a router interconnects two different security zones:

1. Wide Area Network (WAN) zone outside our security perimeter, which includes:
   - Cellular (LTE) network(s), typically with the Internet access
   - Backup Ethernet connection to another WAN router
2. Local Area Network (LAN) zone inside our security perimeter, which includes:
   - Devices connected to the wired or wireless Ethernet (WiFi)
   - Devices (PLC) connected via the serial link (RS232/RS485)
   - Peer LAN connected via the VPN

The essential function of a cellular router is to preserve confidentiality and integrity of the LAN and its information assets. These functions must be preserved even under a DoS attack, when e.g. availability of the router is degraded.

To meet these needs the Advantech cellular routers provide the following security features:

- **Firewall and NAT** filter incoming and outgoing network traffic based on a set of rules. The stateful firewall can:
  - Allow/deny TCP connections and UDP or ICMP packets based on source and/or destination address and port.
  - Protect against common Denial of Service (DoS) attacks.
- **Cryptographic protection** of WiFi and VPN communication (either OpenVPN or IPsec) prevents unauthorized nodes from connecting and protects integrity and confidentiality of the network traffic.

1.2 Cryptographic algorithms

NIST SP 800-57[1] specifies security algorithms with similar strength and recommends the strength equivalent to 112-bit symmetric keys for years 2019-2030 and the strength of 128-bits beyond 2030 (Table 1). The **bold** values are recommended by ANSSI[2] for 2021-2030 and by BSI[3] for 2020-2022.

Strength	Symmetric Key Algorithms	Asymmetric Key Algorithms			Hash Functions
		Diffie-Hellman	RSA	Elliptic Curves	
<=80		L=1024 N=160	k=1024	f=160-223	SHA-1
112	3DES	**L=2048 N=224**	**k=2048**	f=224-255	SHA-224, SHA-512/224, SHA3-224
128	**AES-128**	L=3072, N=256	k=3072	**f=256-383**	**SHA-256, SHA-512/256, SHA3-256**
192	AES-192	L=7680, N=384	k=7680	f=384-511	SHA-384, SHA3-384
>=256	AES-256	L=15360, N=512	k=15360	f=512+	SHA-512, SHA3-512

Table 1: Strength of cryptographic algorithms per NIST SP 800-57

Strength	Encryption	Diffie-Hellman (DH) Group		Hash
		(Finite-Field) Diffie-Hellman	Elliptic Curve (ECDH)	
<=80		Group 2 (1024-bit MODP) Group 5 (1536-bit MODP)		MD5 SHA1
112	3DES	Group 14 (2048-bit MODP)		
128	**AES 128**	**Group 15 (3072-bit MODP)**	Group 19 (256-bit ECP)	**SHA 256**
152		Group 16 (4096-bit MODP)		
176		Group 17 (6144-bit MODP)		
192	AES 192		Group 20 (384-bit ECP)	SHA 384
200		Group 18 (8192-bit MODP)		
256	AES 256		Group 21 (521-bit ECP)	SHA 512

Table 2: Strength of available IPsec algorithms

The Wi-Fi encryption (WPA2-PSK) uses AES-256. The security strength of various IPsec settings is compared in the Table 2.

The IPsec configuration is often a tradeoff between the security strength and the throughput since more complex algorithms need more CPU power, hence the data throughput becomes lower. The **bold** values indicate the default values used when the **auto** mode is used.

[1] https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/draft

[2] https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

[3] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile

1.3 Integration with external components

The router can operate as a standalone device. However, the following features require a central monitoring and management for better security protection:

- **Remote monitoring** by a network monitor such as PRTG or Zabbix [4] can detect anomalies through a collection and analysis of:
  - Router status information such as connection status, interface statistics or voltage and temperature (SNMP [2]);
  - Significant events on the router such as reboots, user logins or configuration changes (syslog);
  - Inbound and outbound network packet flows (NetFlow/IPFIX [3]).

  For more details please see the *Remote Monitoring* Application Note [1].
- **Automatic Update** ensures the router is running the latest firmware with all available security patches.

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://icr.advantech.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 *Security Guidelines* [2] and verify the router configuration is well hardened.

[1] https://icr.advantech.cz/support/router-models
[2] https://icr.advantech.cz/download/application-notes#security-guidelines

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. Always change the default password, even if the default password is complex.
2. If multiple persons need to access the router, create muliple accounts, one for each person.
3. 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[3] that shows how long it would take a modern computer to crack passwords of varying complexities.

   According to the NIST SP 800-63B[4] the passwords shall be at least 8 characters in length, but no other complexity requirements should be imposed. Research has shown, that users respond in very predictable ways to the requirements imposed by composition rules.

   The password complexity policy may be configured in '/etc/settings.policy':

```
POLICY_PWD_LENGTH=8
POLICY_PWD_UPPERCASES=0
POLICY_PWD_LOWERCASES=0
POLICY_PWD_DIGITS=0
```

4. Make sure complex passwords are used for all user accounts and also for all services used in the device, such as Wi-Fi, SNMP or RADIUS, including services provided by user modules.
5. Never use the same or similar password to other devices or systems.

   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.
6. Keep the password secret. Do not share it with anyone and do not store it in close proximity to the device (e.g. written on a sticker).

[3] https://www.ghacks.net/2012/04/07/how-secure-is-your-password
[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

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*.

By default, only configuration is stored.
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.

Recommendation

1. Use a complex *Encryption Password* (see Section 2.2) for any *Configuration Backup*. It must not be left blank, or set to a trivial value that can be easily guessed.
2. Do not replicate private keys to other devices. Each device should have its own.

2.4 Verify server authenticity

Risk

The first time you connect to a server via **ssh** or **scp**, the client will prompt you with a fingerprint of the server public key:

```
The authenticity of host 'server.com (192.168.1.1)' can't be established.
ECDSA key fingerprint is SHA256:NYo7IfkKOHUNScw3fEJxNKMRU+TZkvXe9UmW4w2dA2I.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

This is to verify authenticity of the server. If you always accept this message without checking, there is a risk you will be actually connected to a fake server operated by an attacker, who will then be able to read your password or files you send to the server.

Recommendation

Always verify the server fingerprint when connecting for the first time to a server. Accept the verification request only when you are absolutely sure the server has not been forged. Ask the system administrator if you don't know the correct fingerprint.

If you are an administrator, maintain a list of SSH fingerprints of your machines such as servers and routers. You can retrieve the fingerprint using the **ssh-keygen** tool.

```
user@server.com:/tmp$ ssh-keygen -l -f ssh_rsa_key
256 SHA256:NYo7IfkKOHUNScw3fEJxNKMRU+TZkvXe9UmW4w2dA2I localhost (ECDSA)
```

Due to size constraints the ssh-keygen is not available on routers, but you can temporarily copy the key to another server.

Related to CVE-2020-14145.

2.5 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 or PRTG) and let it listen for Syslog UDP messages.
2. In the *Syslog* service configuration enter the *Remote IP Address* of the log collection server. We recommend you enter *127.0.0.1* and install the **Secure Syslog User Module** as described in its Application Note [5].
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 (and disconnecting from) the WiFi AP
   - Clients requesting (and releasing) an IP address via DHCP

For more details on remote monitoring please see the *Remote Monitoring* Application Note [1].

2.6 Monitor Network Traffic

Risk

In some deployments is the LAN not under a strict control, e.g. when portable devices such as laptops may be temporarily connected for maintenance reasons. These devices may contain a malicious code, which may endanger the network from inside the security perimeter.

The likelihood of success or damage may be higher if the internal attacks go unnoticed.

Recommendation

A network behaviour analysis can identify unusual traffic flows, such as denial of service attacks, certain forms of malware, such as worms or backdoors, and policy violations, such as excessive network use.

1. Setup a network monitoring system (e.g. PRTG).
2. Deploy the **NetFlow/IPFIX User Module** as described in its Application Note [3].
   - Download the module and *Add* it to your routers in the *User Modules* configuration;
   - In the module cpnfiguration, check *Enable Probe* and enter the IP address of your monitoring system as the *Remote Collector*.

The NetFlow data should not be sent over WAN, unless VPN is used. The data are not inherently encrypted or obfuscated, so an unauthorized person may intercept and view the information.

2.7 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;
    - Consider changing passwords that are similar to those stored in the device;
    - Revoke certificates for all private keys stored on the device.

2.8 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. Use the `shred` tool [6] to securely remove sensitive files, e.g. `shred -u file1.txt`.
3. Delete all remaining sensitive information in /var/data and make sure all data possibly installed by custom user modules or owned by other users have been removed.
4. If you uploaded own HTTPS certificate, *Generate a new certificate* to overwrite your certificate with a generic, self-signed one.
5. Perform Factory Reset by pushing/holding the *RST* button (see the User Manual). Then, wait until the *PWR* LED starts blinking again.
6. Power off the device and remove all SIM cards.
7. Remove all references to the device from network servers like DHCP or DynDNS.

3. Hardening Guide

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

3.1 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 unintentional disconnection. For critical systems use Uninterruptible Power Supplies (UPSs).
3. Protect input and output cabling.

3.2 Keep user login disabled

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** (root), 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 is allowed.

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 regular (non-root) users command line access to the router.

3.3 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

1. 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.
2. With **WPA2-PSK** use either a random **256-bit secret**, or a complex **ASCII passphrase** (as recommended in Section 2.2).
3. With **WPA2-Enterprise** use a complex *RADIUS Auth/Acct Password*.

3.4 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.

3.5 Disable unused services

Weakness

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

Defaults

Most network services are disabled by default. Only the following services are listening (on their default ports) for inbound network communications:

- DHCP server on primary LAN (eth0): udp/67
- DNS: tcp/53 and udp/53
- HTTPS: tcp/443
- SSH: tcp/22
- SNMP: udp/161

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

- HTTP: tcp/80
- FTP: tcp/21
- Telnet: tcp/23

Hardening

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

   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.
3. *Save Report* and in the *Sockets* section review UDP ports and all TCP ports in the LISTEN state. Only enabled services should listen on non-local addresses (other than *::1* and *127.0.0.1*).

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

3.6 Avoid using public IP addresses

Weakness

When the router is accessible using a public IP address, anyone anywhere in the world may try connecting, including cybercriminals. The attack surface gets very broad and the risk of attack increases. For more details read The dangers of public IPs from Kaspersky Daily.

Defaults

By default the router obtains its IP address from the network operator, or (on the eth0 interface) from the DNS server. Quite often the network operators use private networks and protect their customers from unwanted Internet traffic.

Hardening

Don't use public IP addresses; don't make you router accessible from the public Internet. If you need to access your router remotely, you may:

- Setup a VPN (Virtual Private Network), e.g. using Advantech WebAccess/VPN.
- Ask your network operator to setup a private APN for you.

3.7 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). **These settings do not apply to LAN interfaces.**

   Rules are processed sequentially and the first matching rule applies.

   - First define protocols or addresses that pose a threat to your network and must be denied (if any).
   - Then, define trusted protocols and addresses that need to be allowed.
   - Traffic not matching any of these rules will be denied by default.
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, i.e. Maximum Segment Size (allows min 250 bytes)
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

3.8 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.

3.9 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.

3.10 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. In the *NAT* configuration, both *remote HTTP access* and *remote HTTPS access* shall be disabled. The web administration shall not be accessible from the Internet.

Always keep HTTPS enabled. If both HTTP and HTTPS is disabled, the web administration will not be accessible via any interface.

Related to Nessus-26194.

3.11 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.

The latest TLS 1.3 is supported since v6.2.8.

Hardening

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

3.12 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:

- Using RSA keys of at least 2048 bits;
- 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-15901, Nessus-51192, Nessus-57582, Nessus-69551.

3.13 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.

3.14 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. The old SNMP versions should be avoided and used in private LAN only.
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 complex value that cannot be easily guessed, see Section 2.2.

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

3.15 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:

- Allow TCP for selected services
- Deny all other TCP

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

Related to CVE-2008-4609.

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

Related Documents

[1] Remote Monitoring
[2] SNMP Object Identifiers
[3] Router App NetFlow/IPFIX
[4] Zabbix Integration Guide
[5] Secure Syslog
[6] Commands and Scripts

[EP] Product-related documents and applications can be obtained on **Engineering Portal** at `https://icr.advantech.cz/download` address.

Document History

2022-10-11 (1.3.1)	Added recommendation to use the shred tool to *Remove stored data when decommissioning*.
2021-10-01 (1.3.0)	Added recommendation to *Avoid using public IP addresses*. Suggested to use *Secure Syslog* [5] in *Monitor system logs*. Added a list of default open ports to Section 3.5. Recommended RSA keys of at least 2048 bits in *Use a proper HTTPS certificate*. Added reference to TLS 1.3 in *Use secure HTTPS ciphers*. Added a list of subjects covered to the Introduction. Changed ep.advantech-bb.cz to icr.advantech.cz in all links.
2020-11-04 (1.2.0)	Updated after a review by an external security advisor. Modified section ordering and wording for better clarify and comprehension. Added references to the *Remote Monitoring* [1] and *Zabbix Integration* [4]. Emphasized the need for complex passwords through the document and clarified the password complexity policy in *Use complex passwords*. Further explained whitelisting and blacklisting in *Use restrictive firewall*. Discouraged private key replication in *Use encrypted backups*. Added reminder to remove user owned information to *Remove stored data*.
2020-07-31 (1.1.0)	Added links to Security inquiries and reports on the title page. Introduced security zones and described security strengths of supported cryptographic algorithms in *Security Features*. Added a suggestion to monitor DHCP client activities in *Monitor System Logs*. Added the *Verify Server Authenticity* and *Monitor Network Traffic* recommendations. Added a list of *Related Documents* and *Document History*.
2020-05-06 (1.0.0)	Initial release.