DOCUMENT ID: 2NGA001253
REVISION: B
DATE: 2022-06-20

CYBER SECURITY ADVISORY

Arctic Wireless Gateway Firewall vulnerability

CVE ID: CVE-2022-0947

ABBVREP0070- ELDS2202

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

The products listed in the table are affected by the vulnerability.

Product / System line	Products and Affected Versions	Advisory
ABB ARG600 Wireless Gateway series	ARG600A1220NA, ARG600A1230NA, ARG600A1240NA, ARG600A1260NA, ARG600A2622NA, ARG600A2625NA - from firmware version 2.4.0 up to firmware version 3.4.10	Advisory
ABB ARP600 Wireless Gateway series	ARP600A2200NA, ARP600A2220NA, ARP600A2250NA, ARP600A2260NA, ARP600A2651NA, ARP600A2560NA - from firmware version 2.4.0 up to firmware version 3.4.10	
ABB ARR600 Wireless Gateway series	ARR600A3201NA, ARR600A3202NA, ARR600A3221NA, ARR600A3222NA, ARR600A3251NA, ARR600A3252NA, ARR600A3261NA, ARR600A3262NA - from firmware version 2.4.0 up to firmware version 3.4.10	
ABB ARC600 Wireless Gateway series	ARC600A2325NA, ARC600A2323NA, ARC600A2324NA - from firmware version 2.4.0 up to firmware version 3.4.10	

Product / System line	Products and Affected Versions	Advisory
Viola Systems Arctic wireless gateways	All 3G and LTE models - from firmware version 2.4.0 up to firmware version 3.4.10	Advisory

Vulnerability IDs

ABBVREP0070- ELDS2202

CVE-2022-0947

Summary

A vulnerability is found in the ABB Arctic wireless gateways in a specific configuration and when using firmware versions from 2.4.0 or later until the version 3.4.10.

The vulnerability manifests itself when the Ethernet port function is configured as "VLAN" and the interface type of VLAN is configured as "WAN". When the device is running such configuration, the firewall will pass all incoming traffic. Other Ethernet port configurations (where the "port function" is set as "auto", "LAN" or "WAN") are not affected.

Recommended immediate actions

Update the firmware to the version 3.4.11, which completely fixes the vulnerability. If unable to patch the system, perform the following check and in case of a vulnerable system, follow the instructions below.

Inspect whether the combination of port function: "VLAN" and VLAN interface type: "WAN" is used in the configuration of Arctic wireless gateways (i.e., no active "LAN" interface is present). If such a configuration exists, refer to the "Mitigating factors" chapter for suggested actions.

Vulnerability severity and details

A vulnerability exists in the firewall included in the product versions listed above. When using a public IP SIM card, an attacker could exploit the vulnerability by remotely connecting to the serial port gateway, and/or protocol converter, depending on the configuration. The web user interface (WHMI) and command line interface (CLI) of the device are also exposed, enabling e.g., dictionary attacks for discovering user credentials. The same attack surface is also existing for local attacks.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2022-0947 Arctic wireless gateway firewall vulnerability

CVSS v3.1 Base Score: 9.0

[1] The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVSS v3.1 Temporal Score: 8.3
CVSS v3.1 Vector: CVSS:3.1/ AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
NVD Summary Link:
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector= AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H

Mitigating factors

This cybersecurity advisory describes how to mitigate the impact of vulnerability. Refer to section “General security recommendations” for further advise on how to keep your system secure.

By configuring the firewall with the following instructions, the problem can be mitigated. In the procedure, certain firewall's "General" configuration rules that are related to the problem are disabled and user-created rules are respectively configured for allowing the traffic.

1. Create a backup of the current active configuration by exporting it to a PC via Tools -> Configuration profiles -> export. The currently running configuration is marked by “radio button”-style icon in the left side of the configuration profile name.
2. Create the necessary input rules manually in Firewall -> filter incoming. For example, create a new firewall rule for input table "filter incoming" for allowing the TCP 443 (HTTPS) port destined to the IP address required (see the *figure 1* below).

   Note 1: Verify that the IP subnet range in the firewall rule covers the Arctic wireless gateway’s IP address, associated to the VLAN interface.

   Note 2: The incoming interface must not be defined in the rule. If needed, the source IP address or source IP subnet address can be defined.

   Note 3: There is an example rule below for allowing the user to access the WHMI (web human-machine interface) of the device. Replace the *<safe_network>* and *<netmask>* placeholders with the actual values. Create similar rules for other ports to where the access is required, e.g., for SSH port TCP 22, used for command line shell access.
3. Change the “GUI anti-lockout” to “No” in Firewall -> General.
4. Change the “LAN-In accepted” to “No” in Firewall -> General.

   Note 4: If having a LAN devices that are using some service of the Arctic wireless GW (such as NTP, DNS, etc.), create respective additional firewall rule for each service.
5. Reboot the device and verify the functionality.

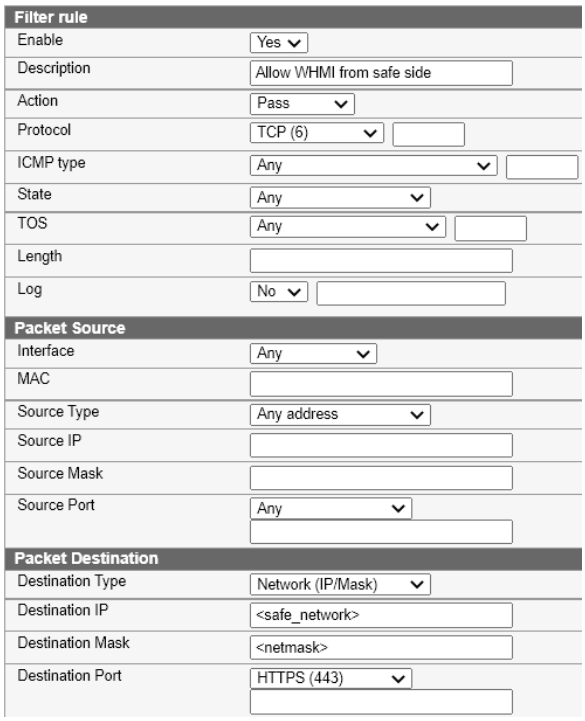

Figure 1: An example firewall rule

Frequently asked questions

What is the scope of the vulnerability?

The firmware versions from 2.4.0 until the version 3.4.10 are vulnerable. The vulnerability is associated to a specific configuration where the Ethernet port function is "VLAN" and the interface type of VLAN is "WAN".

What causes the vulnerability?

There is a flaw in the script that creates the actual iptables firewall rules from the firewall configuration. With certain configuration, too permissive rules are created.

What is the firewall?

In this case, the firewall is an internal software component in the Arctic wireless gateway, which either passes or blocks the traffic based on the security rules.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could gain access to certain functions of the device. Depending on the configuration, such functions would be:

- Serial gateway, IEC-104 gateway, Modbus gateway and/or RTU application (where available and enabled in the product variant)
- Web user interface, command line interface and/or restricted shell (these interfaces are requiring authentication)

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. Alternatively, the attacker could run a dictionary attack against the WHMI or CLI login for trying to get access to the device. The exploit would require that the attacker has access to the system network, by connecting to the network either directly or through a public IP address that the device may have. Recommended practices help mitigate such attacks, refer to section "Mitigating Factors" above.

Could the vulnerability be exploited remotely?

In typical use cases (i.e., when using a consumer-grade SIM card with operator NAT in a public cellular access point or when using a private cellular access point), there is no direct access to the device from internet. An attacker who has network access to the affected system node could exploit this vulnerability. The Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

Can functional safety be affected by an exploit of this vulnerability?

Yes. Depending on the configuration and application, there is a possibility to e.g., operate the inputs/outputs by specially crafted control messages.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g., for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g., office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.

– When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

More information on recommended practices can be found in the following document:

1MRS758860, revision F: Arctic, Cyber Security Deployment Guideline

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	Mar-28-2022
B	p3, c5	Added a solution to update the firmware	Jun-20-2022