DOCUMENT ID: 2NGA002427
REVISION: A
DATE: 2025-04-07

CYBER SECURITY ADVISORY

ABB Arctic ARG600, ARC600, ARR600, ARP600 Arctic Wireless Gateway Modem Module and OpenSSH vulnerabilities

CVE ID:
CVE-2023-47610, CVE-2023-47611,
CVE-2023-47612, CVE-2023-47613,
CVE-2023-47614, CVE-2023-47615,
CVE-2023-47616, CVE-2024-6387

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

1. CVEs: CVE-2023-47610, CVE-2023-47611, CVE-2023-47612, CVE-2023-47613, CVE-2023-47614, CVE-2023-47615, CVE-2023-47616 concerning the following variants:

   Arctic Wireless Gateways ARG600, ARC600, ARR600 with Telit PLS62-W wireless modem module. Other variants are not affected.

2. CVE-2024-6387 concerning all variants:

   Arctic ARG600, ARC600, ARR600, ARP600 with firmware versions 3.4.10, 3.4.11, 3.4.12, 3.4.13.

Vulnerability IDs

CVE-2023-47610, CVE-2023-47611, CVE-2023-47612, CVE-2023-47613, CVE-2023-47614, CVE-2023-47615, CVE-2023-47616, CVE-2024-6387

Summary

ABB is aware of public reports of the vulnerabilities in the product versions listed above.

An attacker who successfully exploited modem module vulnerabilities could run arbitrary code in the wireless modem module of the product. This could lead to denial of service or tampering with unencrypted traffic.

An attacker who successfully exploited the OpenSSH vulnerability could run arbitrary code in the product with privileged user permissions. This could cause the product to stop, make the product inaccessible, or the attacker could take control of the product.

As part of ABB product lifecycle policy, once a product transitions to Limited state, we discontinue maintenance, security patches, and technical support to focus on current and future technologies. While the product will continue to function, we strongly recommend implementing mitigations defined in this document to mitigate security risks.

Recommended immediate actions

ABB recommends that customers should perform actions described in chapter *Mitigating factors* at earliest convenience.

Vulnerability severity and details

There are vulnerabilities in the Telit PL62-W wireless modem module used in the products listed above. An attacker could exploit these vulnerabilities by e.g., sending a specially crafted message to the system node and running arbitrary code in the wireless modem module, allowing the attacker to cause unwanted behavior in the product.

In addition, there is a vulnerability in OpenSSH software component, where an unauthenticated attacker could exploit the vulnerability by sending a specially crafted message to the system node and executing arbitrary code as privileged user.

A review of the reported CVSS scores has identified discrepancies between the originally assigned vulnerability ratings and the actual impact within the product's security context. CVSS scores are generally determined based on broad risk assessments, but severity can vary depending on factors such as product architecture, configurations, and specific usage scenarios. Therefore, the CVSS scores are adjusted according to the product's security context.

CVE number	CVSS v4.0 score	CVSS v3.1 score	Vulnerability	Exploit type	Exploit method
CVE-2023-47610	9.2	8.1	Buffer Copy without Checking Size of Input	Remote code execution	Remote
CVE-2023-47611	5.4	6.8	Improper Privilege Management	Elevation of privileges	Local *)
CVE-2023-47612	5.4	6.8	Files or Directories Accessible to External Parties	Leaking of sensitive data	Local *)
CVE-2023-47613	2.4	3.2	Relative Path Traversal	Leaking of sensitive data	Local *)
CVE-2023-47614	2.4	3.2	Exposure of Sensitive Information to an Unauthorized Actor	Leaking of sensitive data	Local *)
CVE-2023-47615	5.1	4.3	Exposure of Sensitive Information Through Environmental Variables	Leaking of sensitive data	Local *)
CVE-2023-47616	5.1	4.6	Exposure of Sensitive Information to an Unauthorized Actor	Leaking of sensitive data	Local *)

CVE-2024-6387	9.2	8.1	Race condition in signal handler	Remote code execution	Remote

Table 1: Vulnerabilities

*) Requires physical manipulation of the product.

CVE-2023-47610

A buffer overflow vulnerability that could allow a remote unauthenticated attacker to execute arbitrary code on the targeted system by sending a specially crafted Short Message Service (SMS) message.

CVSS v3.1 Base Score: 8.1
CVSS v3.1 Temporal Score: 7.4
CVSS v3.1 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C

CVSS v4.0 Score: 9.2
CVSS v4.0 Vector: AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:P/AU:Y/R:U/V:D/RE:H/U:Amber

CWE: 120
NVD Summary Link: NVD - CVE-2023-47610

CVE-2023-47611

Improper Privilege Management vulnerability that could allow a local that could allow a local, low privileged attacker to elevate privileges to "manufacturer" level on the targeted system by sending a specially crafted SMS message.

CVSS v3.1 Base Score: 6.8
CVSS v3.1 Temporal Score: 6.0
CVSS v3.1 Vector: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:R

CVSS v4.0 Score: 5.4
CVSS v4.0 Vector: AV:P/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:D/RE:L/U:Amber

CWE: 269
NVD Summary Link: NVD - CVE-2023-47611

CVE-2023-47612

Files or Directories Accessible to External Parties vulnerability that could allow an attacker with physical access to the target system to obtain a read/write access to any files and directories on the wireless modem module, including hidden files and directories.

CVSS v3.1 Base Score: 6.8
CVSS v3.1 Temporal Score: 6.0
CVSS v3.1 Vector: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:R

CVSS v4.0 Score: 5.4

CVSS v4.0 Vector: AV:P/AC:H/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:D/RE:L/U:Ambe

CWE: 200
NVD Summary Link: NVD - CVE-2023-47612

CVE-2023-47613

Relative Path Traversal vulnerability that could allow a local, low privileged attacker to escape from virtual directories and get read/write access to protected files on the wireless modem module.

CVSS v3.1 Base Score: 3.2
CVSS v3.1 Temporal Score: 2.9
CVSS v3.1 Vector: AV:P/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:P/RL:W/RC:R

CVSS v4.0 Score: 2.4
CVSS v4.0 Vector: AV:P/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:D/RE:M/U:Amber

CWE: 22
NVD Summary Link: NVD - CVE-2023-47613

CVE-2023-47614

Exposure of Sensitive Information to an unauthorized actor vulnerability that could allow a local, low privileged attacker to disclose hidden virtual paths and file names on the wireless modem module.

CVSS v3.1 Base Score: 3.2
CVSS v3.1 Temporal Score: 2.9
CVSS v3.1 Vector: AV:P/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:P/RL:W/RC:R

CVSS v4.0 Score: 2.4
CVSS v4.0 Vector: AV:P/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:D/RE:M/U:Green

CWE: 200
NVD Summary Link: NVD - CVE-2023-47614

CVE-2023-47615

Exposure of Sensitive Information Through Environmental Variables vulnerability that could allow a local, low privileged attacker to get access to sensitive data on the wireless modem module.

CVSS v3.1 Base Score: 4.3
CVSS v3.1 Temporal Score: 3.8
CVSS v3.1 Vector: AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:W/RC:R

CVSS v4.0 Score: 5.1
CVSS v4.0 Vector: AV:P/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/S:N/AU:N/R:A/V:D/RE:L/U:Green

CWE:	200
NVD Summary Link:	NVD - CVE-2023-47615

CVE-2023-47616

Exposure of Sensitive Information to an unauthorized actor vulnerability that could allow an attacker with physical access to the target system to get access to sensitive data on the wireless modem module.

CVSS v3.1 Base Score:	4.6
CVSS v3.1 Temporal Score:	4.1
CVSS v3.1 Vector:	AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:W/RC:R
CVSS v4.0 Score:	5.1
CVSS v4.0 Vector:	AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/S:N/AU:N/R:A/V:D/RE:L/U:Green
CWE:	200
NVD Summary Link:	NVD - CVE-2023-47616

CVE-2024-6387

The vulnerability is a signal handler race condition in OpenSSH's server (sshd) on glibc-based Linux systems, allowing unauthenticated remote code execution (RCE) as root.

CVSS v.3.1 Base Score:	8.1
CVSS v.3.1 Temporal Score:	7.1
CVSS v3.1 Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:R
CVSS v4.0 Score:	9.2
CVSS v4.0 Vector:	AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:P/AU:Y/R:U/V:D/RE:M/U:Amber
CWE:	362
CVSS v3.1 Summary Link:	NVD - CVE-2024-6387

Mitigating factors

The following mitigations can be considered

- Obtain a private cellular access point to limit impact of any potential exploit. Contact your cellular provider for availability.
- Mitigate the cellular module vulnerabilities by contacting the mobile network operator and requesting to disable binary SMS for your mobile subscription.
    - Note that binary SMS service is often disabled by default based on operator restrictions.
    - If SMS services are not used in the solution, consider disabling them completely.
- Establish remote connections through OpenVPN. If the SSH protocol is used for remote administration of Arctic wireless gateway, it is to be considered logging in to the wireless gateway through an OpenVPN tunnel.

- Do not expose SSH port to public networks. Keep the SSH port closed to public networks and thus limit the number of potential attackers who can attempt to exploit the vulnerability. This way only devices within your private network or those connected through a secure VPN can access the SSH server.

- Restrict physical access to the product.

Refer to section *General security recommendations* for further advice on how to keep your system secure.

Frequently asked questions

What causes the vulnerabilities?

There are multiple vulnerabilities identified in the cellular modem module; however, the main vulnerability is caused by buffer copy without checking the size of input in the LTE Telit PL62-W modem module.

The SSH vulnerability is caused by a signal handler race condition in OpenSSH's server (sshd).

What is Telit PL62-W?

The PL62-W is a multi-band LTE module developed by Telit. This module provides efficient LTE connectivity across multiple frequency bands and offers fallback to 3G and 2G networks when LTE is not available. It is one of the modem modules used in ABB Arctic ARG600, ARC600, ARR600 Arctic Wireless Gateway products.

What is OpenSSH?

OpenSSH (Open Secure Shell) is a suite of secure networking utilities based on the Secure Shell (SSH) protocol, which is used for secure communication over unsecured networks.

What might an attacker use the vulnerabilities to do?

The cellular modem module vulnerabilities could allow a remote unauthenticated attacker to e.g., execute arbitrary code on the modem module by sending a specially crafted SMS message. In ABB Arctic wireless gateway scope, an attacker could e.g., cause a denial-of-service situation by rendering the cellular modem module inoperable or perform man-in-the-middle attack to unencrypted data transferred through the product.

An attacker who successfully exploited the OpenSSH vulnerability could cause the product to stop, make the product inaccessible, or take control of the product.

How could an attacker exploit the cellular modem module vulnerability?

The cellular modem module vulnerabilities consist of several attack methods, but the main vector is CVE-2023-47610, which is remotely exploitable. A flaw in the modem module's Open Mobile Alliance (OMA) Secure User Plane Location (SUPL) message handler is used for executing arbitrary code that is injected to the device using SMS messages. This allows subsequent fetching of malware payload through Over the Air (OTA) services.

How could an attacker exploit the OpenSSH vulnerability?

There are three scenarios, depending on the type of installation of the Arctic wireless gateway:

Public IP SIM card
When the device is equipped with SIM card subscription assigned with public IP address, it is visible on the Internet. If the SSH port is configured as open in the wireless WAN side, the attacker could exploit the vulnerability and take control of the product. The attack can be automated to search for open SSH ports on the internet.

Private IP SIM card
When the device is equipped with a private IP SIM card subscription, the attacker could only exploit the vulnerability by first using some other weakness for attacking the cellular provider's network or customer's own network.

Most consumer-grade SIM card subscriptions are using private IP addresses or carrier-grade NAT (network address translation) IP addresses that are assigned to the SIM cards. There is a NAT used when the device is connecting to the Internet. Because of the NAT, the devices equipped with private IP SIM card subscription are not visible on the internet (unless a connection to the Internet is opened by the wireless gateway itself) and thus cannot be directly attacked.

Private APN
When a private cellular access point is used, the device is not visible on the Internet and the traffic is never routed over the Internet. Thus, the attacker could only exploit the vulnerability by first using some other weakness for attacking the cellular provider's network or customer's own network.

Recommended practices help mitigate such attacks, refer to section *Mitigating factors* above.

Could the vulnerable products be exploited remotely?

An attacker who has network access to the vulnerable product could exploit the CVE-2023-47610 and CVE-2024-6387 vulnerabilities. Other vulnerabilities mentioned are not remotely exploitable.

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

Yes, if the attacker can e.g., render the wireless connection inoperable and the device is used in a critical application, such as controlling a circuit breaker.

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

Yes, these vulnerabilities have been publicly disclosed.

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

No, ABB had not received information indicating this vulnerability was exploited when this security advisory was 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.

References

1MRS758860, Rev. 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	Apr-07-2025