DOCUMENT ID: 9AKK108467A0927
REVISION: A
DATE: 2022-07-14

CYBER SECURITY ADVISORY

ABB Flow Computer and Remote Controllers Path Traversal Vulnerability in Totalflow TCP protocol can lead to root access
CVE ID: CVE-2022-0902

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.

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 following table lists the flow computer and remote controller products affected by this vulnerability. Note that all products versions (too many to list) prior to the listed flash part numbers are affected.

ABB device	Fixed flash part number	Affected flash part number
RMC-100 (Standard)	2105457-037	All prior to fixed version.
RMC-100-LITE	2106229-011	All prior to fixed version.
XIO	2106198-008	All prior to fixed version.
XFC^{G5}	2105805-016	All prior to fixed version.
XRC^{G5}	2105864-016	All prior to fixed version.
uFLO^{G5}	2105298-024	All prior to fixed version.
UDC	2106177-007	All prior to fixed version.

Vulnerability IDs

CVE-2022-0902

Summary

ABB is aware of private reports of a vulnerability in the flow computer and remote controller product versions listed above.

A flash update is available that resolves the vulnerability in the product versions listed above.

Mitigation can be accomplished by proper network segmentation.

Recommended immediate actions

ABB recommends that customers apply the flash update at the earliest convenience.

Vulnerability severity and details

A path traversal vulnerability exists in the implementation of the Totalflow TCP protocol in ABB G5 products (see the Affected products section for detailed list).

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

CVE-2022-0902 Path Traversal Vulnerability in ABB Flow Computers and Remote Controllers' Totalflow TCP protocol can lead to root access

A path traversal vulnerability can allow unauthenticated users to gain access to restricted directories. Exploiting this vulnerability can lead to pre-authenticated remote code execution in root context.

CVSS v3.1 Base Score:	8.1
CVSS v3.1 Temporal Score:	7.7
CVSS v3.1 Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
NVD Summary Link:	http://nvd.nist.gov/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C

Mitigating factors

To mitigate this vulnerability the ABB device should only be connected to a network segment that restricts access to authorized users. The vulnerability is only exposed when the attacker has access to the network where the ABB device is running Totalflow TCP protocol.

Refer to section General security recommendations for further advise on how to keep your systems secure.

Workarounds

ABB has tested the following workaround. Although this workaround will not correct the underlying vulnerability, it can help block known attack vectors:

[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.

– Isolate the ABB device's network connection to a trusted network segment.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could insert and run arbitrary code in an affected system node.

What causes the vulnerability?

The vulnerability is caused by unchecked input data in the protocol in the G5 products.

What is affected product?

The firmware for the devices listed in the Affected products section of this document.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could allow the attacker to insert and run arbitrary code.

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. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. 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.

What does the update do?

The update removes the vulnerability by modifying the way that the Totalflow protocol validates messages and verifies input data

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.

Acknowledgement

ABB thanks Vera Mens at Claroty Research for helping to identify the vulnerabilities and protecting our customers.

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	2022-7-14