DOCUMENT ID: 2NGA001574
REVISION: A
DATE: 2023-03-07

CYBER SECURITY NOTIFICATION

# ABB Substation management unit COM600 IEC-104 protocol stack vulnerability

ABBVREP0076

## 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 cyber security program which involves not only internal processes to ensure product security but also external engagement with the wider cybersecurity community and 3rd party suppliers. Occasionally an issue is identified with the potential to impact ABB products and systems.

Generally, this means 3rd party product vulnerabilities or life-cycle issues to which ABB products may have a dependency on. Another example could be threats which are not directly targeting ABB products however may constitute a threat to environments where ABB products/systems operate.

When a potential threat is identified or reported, ABB immediately initiates our vulnerability handling process. This entails an evaluation to determine if there are steps which can be taken to reduce risk and maintain functionality for the end user.

The result may be the publication of a Cyber Security Notification. This intends to notify customers of the issue 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 Notification should not be assumed as an 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 Notification is an example of ABB's commitment to the user community in support of this critical topic. The release of a Notification intends to provide timely information which is essential to help ensure our customers are fully informed. See details below and refer to the section on "General security recommendations" for further advise on how to keep your systems secure.

# Background

On Sept-6-2022, vulnerability CVE-2022-29492 was made public by Hitachi Energy. In addition to Hitachi's products defined in the CVE-2022-29492, this vulnerability affects the IEC 68070-5-104 (IEC-104) protocol stack of ABB Substation Management Unit COM600.

Subsequently, a successful exploit could allow attackers to cause a denial-of-service attack against the COM600 product. Exploiting this vulnerability requires the attacker to have network access to the COM600 device directly or via exploited remote connection.

# Related products

ABB has identified that the COM600 product firmware versions

2.x, 3.x, 4.x and 5.x

are affected.

# Recommended immediate actions

- Define the IP address(es) of the allowed IEC-104 client(s). This will exclude other clients from accessing the device.
    - Set the Internet Address(es) (IA) in device properties according to IEC-104 client IP address(es)

- Verify that the "Operating mode" (OM) property of the subnetwork object is set as "Allow connection from specified IP address".

ABB additionally recommends following the instructions in chapters "Mitigating factors" and "General security recommendations" for keeping the system protected.

# Mitigating factors

Since the vulnerability is related to the way how the IEC 60870-5-104 protocol is designed and the implementation of the COM600 IEC-104 stack is according to the specification, the mitigating factors are primarily consisting of reducing the external attack surface to the minimum by, e.g., segregating the network, isolating the network to the degree possible and disabling functionalities and network services, where applicable. See the chapter "General security recommendations" for more details.

# Vulnerability Details

A vulnerability exists in the handling of a malformed IEC 104 TCP packet. The malformed packet is dropped upon receiving a malformed IEC 104 TCP packet. However, the TCP connection is left open. This may cause a denial of service if multiple malformed packets are sent.

**CVE-2022-29492**

CVSS v3.1 Base Score: 5.3 (Medium)

CVSS v3.1 Temporal Score: 5.0

CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:F/RL:W/RC:C

CVSS v3.1 Vector Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:F/RL:W/RC:C

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2022-29492

# General security recommendations

For any installation of software-related ABB products, we strongly recommend the following (non-exhaustive) list of cybersecurity 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 programming 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 designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date regarding installed software, operating system, firmware patches, and 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. Also, understand that VPNs are only as secure as connected devices.

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

1MRS758267, COM600 series 5.1 , 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 | March-07-2023 |
| | | | |
| | | | |