DOCUMENT ID: 7PAA001023
REVISION: B
DATE: 2023-10-12
SECURITY LEVEL: PUBLIC

CYBER SECURITY ADVISORY

SECURITY - Denial of Service Vulnerabilities in System 800xA, Symphony® Plus IEC 61850 communication stack

CVE ID: CVE-2021-27196

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 (e.g. ICS-CERT).

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

Product / System line	Products and Affected Versions
PM 876 (for AC 870P)[1] **PM 876-1 (for AC 870P)**	Firmware versions prior to 2.37
CI850 (for SPC family and HPC800)	Firmware versions prior to A_3
CI868 (for AC 800M)[1]	Firmware versions prior to 6.1.1004.0 (Sytem 800xA version 6.1.1)
S+ Operations[2]	Versions prior to 3.3 SP1 using IEC 61850 connectivity are affected. Versions prior to 2.1.2 using IEC 61850 connectivity are affected.

Vulnerability IDs

CVE-2021-27196

[1] PM 876 and PM 876-1 for S+ Melody and CI868 for System 800xA.

[2] Version 2.1.1 does not support IEC 61850 connectivity and therefore is not affected.

Summary

A vulnerability was privately reported relating to ABB's implementation of the IEC 61850 communication stack used in some Process Automation control system products. If an attacker gains access to a site's IEC 61850 network, then exploiting this vulnerability will result in a device fault (PM 876, PM 876-1, CI850 and CI868 modules) and will require a manual restart.

If this attack is directed at a S+ Operations node running IEC 61850 connectivity, this will result in a crash in the IEC 61850 communication driver which, if continued on a repeating basis, will also result in a denial-of-service situation. Note that this does not impact the overall availability and functionality of the S+ Operations node, only the IEC 61850 communication function. The System 800xA IEC61850 Connect is not affected.

Recommended immediate actions

ABB advises all customers to review their installations to determine if they are using an impacted product as listed above, no further analysis or tools are needed to make this determination. The recommended immediate actions per product are listed below:

- **PM 876 and PM 876-1 (for AC870P)**

  Upgrade to FW version 2.37 (released 2016) or later where the affected port is disabled in firmware.

  Note: For PM877 no action is required. The affected port is already disabled in firmware.

- **CI850 (for SPC family and HPC800)**

  Upgrade firmware to version A_3 or later (released in December 2022).

- **CI868 (for AC 800M)**

  Systems using 800xA version 6.1.0 or earlier should be upgraded to version 6.1.1 or later.

  Systems using 800xA LTS version 6.0.3.3 or earlier should be upgraded to 6.0.3.4 (released in October 2022).

  Systems using 800xA version 5.1 or earlier should be upgraded to version 6.1.1.

- **S+ Operations**

  Systems using S+ Operations versions 2.0.x and 2.1[3] should upgrade at least to version 2.1 SP2 or directly to version 3.3 SP1 or later.

  Systems using S+ Operations version 3.1, 3.2 or 3.3 should upgrade to version 3.3 SP1 or later.

  Note: If the IEC 61850 connectivity is not licensed, i.e. not used, the driver cannot run and S+ Operations is not affected. No further actions are required in this case.

End users who are unable to install one of these updates should immediately look to implement the Mitigation and Workarounds listed below as this will restrict or prevent an attacker's ability to compromise these systems.

[3] Versions 2.1.1 and 2.2 do not support IEC 61850 connectivity and therefore is not affected.

Vulnerability severity and details

A vulnerability exists in the command handling of the IEC 61850 communication stack included in the product revisions listed above. An attacker with access to IEC 61850 networks could exploit the vulnerability by using a specially crafted 61850 packet to port 102, forcing the communication interfaces of the PM 876, PM 876-1, CI850 and CI868 modules into fault mode or causing unavailability of the S+ Operations 61850 connectivity, resulting in a denial-of-service situation. The System 800xA IEC61850 Connect is not affected.

Note: This does not impact the overall availability and functionality of the S+ Operations node, only the 61850 communication function.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[4].

CVE-2021-27196 - Improper Input Validation

CVSS v3.1 Base Score:	7.5 (High)
CVSS v3.1 Temporal Score:	7.2 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2021-27196

Mitigating factors

The vulnerabilities announced in this Advisory for ABB Process Automation products require that an attacker has access to the system network and hosts which are generally expected to be protected.

Process Control and IEC 61850 networks are NOT recommended to be exposed directly to Internet connections. If these networks are not properly isolated, then connected components may be remotely exploitable as described in this advisory.

To exploit the vulnerability an attacker with remote network access can send a specially crafted packet to port 102 of the PM 876, PM 876-1, CI850 and CI868 which causes the fault of these devices. Therefore, use of a perimeter firewall to block port 102 is an effective mitigation.

Note: S+ Operations only implements 61850 client services and therefore are not intended to listen on port 102. However, if a specially crafted message is sent anyway it can still cause the 61850 communication driver to crash. Therefore, enabling the Windows firewall and ensuring port 102 is blocked is an effective mitigation.

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

[4] 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.

Workarounds

Isolate IEC 61850 networks from all external network connections.

Frequently asked questions

What is the scope of the vulnerability?

An attacker having access to the IEC 61850 network can force the ABB hardware devices to go to 'fault' state by sending a specially crafted message sequence. This will result in a denial of service situation affecting the primary functionality of the listed devices and requiring a manual reset. In the same way this vulnerability can cause the unavailability of the S+ Operations 61850 connectivity (but not the whole S+ Operations node). The System 800xA IEC61850 Connect is not affected.

What causes the vulnerability?

The vulnerability is caused by a weakness in the message processing in the IEC 61850 communication stack.

What is the IEC 61850 Communication Stack?

The IEC 61850 stack included in the Affected products listed above is the ABB software implementation of the IEC 61850 communication stack.

What might an attacker use the vulnerability to do?

An attacker with access to IEC 61850 networks could exploit the vulnerability by using a specially crafted 61850 packet to port 102, forcing the Communication Interfaces to fault modes or causing unavailability of the S+ Operations 61850 connectivity, resulting in a denial-of-service situation.

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.

Could the vulnerability be exploited remotely?

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

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

Functional safety systems are not affected by these vulnerabilities.

What does the update do?

The update removes the vulnerability by modifying the way that the IEC 61850 stack, used by the ABB Process Automation Products described above, manages 61850 incoming 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

Control systems and the control network are exposed to cyber threats. In order to minimize these risks, the protective measures and best practices listed below are available in addition to other measures. ABB strongly recommends system integrators and asset owners to implement the measures they consider appropriate for their control system environment:

– Place control systems in a dedicated control network containing control systems only.

– Locate control networks and systems behind firewalls and separate them from any other networks like business networks and the Internet.

– Block any inbound Internet traffic destined for the control networks/systems. Place remote access systems used for remote control system access outside the control network.

– Limit outbound Internet traffic originating from control systems/networks as much as possible. If control systems must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which control systems definitely need to use for normal control operation.

– If Internet access is required on occasion only, disable relevant firewall rules and enable them during the time window of required Internet access only. If supported by your firewall, define an expiry date and time for such rules – after the expiry date and time, the firewall will disable the rule automatically.

– Limit exposure of control networks/systems to internal systems. Tailor firewall rules allowing traffic from internal systems to control networks/systems to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal control operation.

– Create strict firewall rules to filter malicious network traffic targeting control system vulnerabilities ("exploit traffic"). Exploit traffic may use network communication features like source routing, IP fragmentation and/or IP tunneling. If such features are not required for normal control operation, block them on your firewall.

– If supported by your firewall, apply additional filters to allowed traffic which provide protection for control networks/systems. Such filters are provided by advanced firewall features like Application Control and Anti-Virus.

– Use Intrusion Detection Systems (IDS) or Intrusion Preventions Systems (IPS) to detect/block control system-specific exploit traffic. Consider using IPS rules protecting against control system exploits.

– When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please ensure that VPN solutions are updated to the most current version available.

– In case you want to filter internal control network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.

– Harden your control systems by enabling only the ports, services and software required for normal control operation. Disable all other ports and disable/uninstall all other services and software.

- If possible, limit the permissions of user accounts, software processes and devices to the permissions required for normal control operation.
- Use trusted, patched software and malware protection solutions. Interact with trusted web sites and trusted email attachments only.
- 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.
- Protect control systems from physical access by unauthorized personnel e.g. by placing them in locked switch cabinets.

More information on recommended practices can be found in the following documents[5]:

2VAA000585	S+ Control PM 876 User Manual
2VAA003700	S+ I/O: SD Series I/O: CI850 IEC 61850 Communication Module and Hardware Operation User Manual
8VZZ001882	S+ Control SPC600/700/800 SD Series controllers user manual
9ARD171385-611	System 800xA 6.1.1 AC 800M - IEC 61850 Configuration for CI868
8VZZ001006	Symphony Plus Secure deployment guide for Windows 10 and Server 2016/2019 user manual
2PAA121027	Distributed Control Systems - McAfee® ePO with VirusScan Enterprise, Endpoint Security and Application Control
8VZZ000602	Microsoft Security Updates Validation Status for Symphony Plus
8VZZ001753	McAfee Virus Scan DAT Update Validation Status for Symphony Plus
2PAA122516	System 800xA, Symphony Plus and Freelance System Hardening - End user manual
2PAA120528	System 800xA, Symphony Plus and Freelance System Hardening: Group Policies Overview
8VZZ000368D0066	ICS Cyber Security Reference Architecture Guide

Acknowledgement

ABB thanks Hitachi Energy (formerly Hitachi ABB Power Grids) for sharing the information affecting a commonly used software component (CVE-2021-27196) as well as the original finders at GAI netConsult.

Support

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

[5] Access to some listed documents can be subject to the ABB Care Automation Software Maintenance specific conditions and agreements.

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	2021-12-21
B	Page 3	Updated released dates for CI850 and CI868	2023-10-12