DOCUMENT ID: 7PAA020125
REVISION: B
DATE: 04/10/2026

SECURITY ADVISORY

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

CVE ID: CVE-2025-3756

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
CI868	Module used in AC800M product line (System 800xA) for IEC 61850 communication. The affected firmware versions are: • 6.0.0303.0 and earlier (AC800M version 6.0.0-x) • 6.1.0031.0 and earlier (AC800M version 6.1.0-x) • 6.1.1004.0 and earlier (AC800M version 6.1.1-0 and 6.1.1-1) • 6.1.1202.0 and earlier (AC800M version 6.1.1-2) • 6.2.0006.0 and earlier (AC800M version 6.2.0-0)
CI850	Module used in Symphony Plus SD Series product line for IEC 61850 communication. The affected firmware versions are: • A_0 • A_1 • A_2.003 • A_3.005 • A_4.001 • B_0.005
PM 877	Module used in Symphony Plus MR (Melody Rack) product line for IEC 61850 communication. The affected firmware versions are: • from 3.10 till 3.52

Product / System line	Products and Affected Versions
S+ Operations	S+ Operations using IEC 61850 connectivity. The affected versions are: • 3.3 and related Service Packs • 2.3 • 2.2 and related Service Packs • 2.1 and related Service Packs

Vulnerability IDs and Product Issue Numbers (PIN)

CVE-2025-3756

Summary

A vulnerability was privately reported relating to ABB's implementation of the IEC 61850 communication stack for MMS client applications used in some Automation control system products.

Note: IEC 61850 communication typically supports MMS and GOOSE protocols. Some ABB products support both, others only MMS (e.g. S+ Operations and PM 877). In any case, GOOSE communication is not impacted by this reported vulnerability.

If an attacker gains access to a site's IEC 61850 network, then exploiting this vulnerability will result in a device fault (PM 877, 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 a repeating basis, will also result in a denial-of-service situation. Note that this does not have an impact on 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:

– **CI868 (for AC 800M)**
Devices with firmware versions reported in Affected products are vulnerable. All the vulnerabilities will be corrected in 6.1.1[1] and 7.0 tracks for 800xA. AC 800M 6.1.1-3 is planned for Q2 2027, AC 800M 7.0 has been released in December 2025.

[1] The fix for 6.1.1 will be achieved by an update to 6.1.1 which will be released in 2027 as mentioned, the fix for version 6.2 is achieved by upgrading to version 7.0.0-0, as version 6.2 is a continuous release version according to the DCS life cycle policy.

- **CI850 (for Symphony Plus SD Series)**
  Devices with firmware versions reported in Affected products are vulnerable. All the vulnerabilities will be corrected in version C_0 or later (planned Q2 2026).
- **PM 877 (Symphony Plus MR)**
  Devices with firmware versions reported in Affected products are vulnerable. All the vulnerabilities will be corrected with firmware version 3.53 or later (planned Q1 2026).
- **S+ Operations**
  Versions reported in Affected products are vulnerable. All the vulnerabilities will be corrected in version 3.4 or later (released in January 2026).

ABB recommends customers apply updates, as they become available, at their earliest convenience. It is also advisable to review the Mitigating Factors, Workarounds and General security recommendations sections for additional actions which may help reduce overall risk.

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, forcing the communication interfaces of the PM 877, 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 vulnerability does not impact on 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)[2] for both v3.1[3] and v4.0[4].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[5].

CVE-2025-3756 Improper Handling of Variables in IEC 61850 MMS Report

CVSS
CVSS v3.1 Base Score: 6.5 (Medium)
CVSS v3.1 Temporal Score: 6.5 (Medium)

[2] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., https://www.first.org/cvss/.

[3] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. 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.

[4] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

[5] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

CVSS v3.1 Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Score: 7.1 (High)
CVSS v4.0 Vector: CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE
CWE-1284: Improper Validation of Specified Index, Position, or Offset in Input.

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-3756

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 the PM 877, CI850 and CI868 modules which causes the fault of these devices.

S+ Operations only implements 61850 client services and therefore are not intended to listen to incoming connection requests. However, if a specially crafted message is sent anyway, it can still cause the 61850-communication driver to crash.

The usage of a perimeter firewall to allow legitimate client communications is an effective mitigation.

Refer to section “General Security Recommendation” for further advise on how to keep your system secure.

Workarounds

No workarounds are available. Assess the installation specific risk based on this advisory. Use the recommendations described under “Mitigating factors” or “Recommended immediate actions”.

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 61850 packet. 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, if continued on a repeating basis (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 CI868?

CI868 is a module used in AC800M product line (System 800xA) for IEC 61850 communication.

What is CI850?

CI850 is a module used in Symphony Plus SD Series product line for IEC 61850 communication.

What is PM 877?

PM 877 is a controller used in Symphony Plus MR (Melody Rack) product line for IEC 61850 communication.

What is S+ Operations?

S+ Operations is the Human Machine Interface for supervision and control of Symphony based control or SCADA systems.

What might an attacker use the vulnerability to do?

An attacker with access to IEC 61850 networks could exploit the vulnerability by sending a specially crafted 61850 packet to the S+ products, 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. 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.

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. 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 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[6]:

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
8VZZ001006T0001	Symphony Plus Secure deployment guide for Windows 10 and Server 2016/2019 User manual
2PAA121027	Distributed Control Systems Trellix ePO with Endpoint Security and Application Control - Configuration Manual
8VZZ000602	Symphony Plus Security Updates Validation Status
7PAA018617	Symphony Plus Daily Validation of Anti-Malware Definition Updates

Acknowledgement

ABB thanks Hitachi Energy for sharing the information affecting a commonly used software component.

References

2PAA122516	System 800xA, Symphony Plus and Freelance - System Hardening - End user manual
8VZZ000368D0066	ABB ICS Cyber Security Reference Architecture - Document

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.

[6] Access to listed documents might be restricted to customers having an active ABB Care Automation Software Maintenance agreement and a valid ABB MyControlSystem user ID.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	04/10/2026
B	P7	Corrected typos in the FAQ	04/13/2026