DOCUMENT ID: 7PAA017341
REVISION: A
DATE: 04/10/2026

CYBER SECURITY ADVISORY

PostgreSQL vulnerabilities in ABB Ability™ Symphony® Plus Engineering

CVE ID: CVE-2023-5869, CVE-2023-39417, CVE-2024-7348, CVE-2024-0985

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 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

ABB Ability™ Symphony® Plus:

- S+ Engineering 2.2
- S+ Engineering 2.3, 2.3 RU1, 2.3 RU2 and 2.3 RU3
- S+ Engineering 2.4, 2.4 SP1 and 2.4 SP2

Vulnerability IDs

CVE-2023-5869, CVE-2023-39417, CVE-2024-7348, CVE-2024-0985

Summary

The ABB S+ Engineering product versions listed above are affected by vulnerabilities in PostgreSQL version 13.11 and earlier versions. If an attacker gains access to a site's S+ Client Server network, they could exploit such vulnerabilities by executing arbitrary code and potentially compromising the entire system.

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:

Systems using S+ Engineering 2.2 through 2.4 SP2 should upgrade to S+ Engineering 2.4 SP2 RU1 (released in December 2024) or later.

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 the system.

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

Vulnerability severity and details

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

CVE-2023-5869 Missing Integer Overflow Check

An attacker running as an authenticated PostgreSQL user can provide crafted data and trigger the integer overflow due to such missing overflow check. This can enable the execution of arbitrary code in the system.

CVSS v3.1 Base Score: 8.8 (High)
CVSS v3.1 Temporal Score: 8.8 (High)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE
CWE-190 - Integer Overflow or Wraparound.

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-5869

CVE-2023-39417 SQL Injection in Extension Script

If an administrator has installed Extension scripts and specific data is used inside a quoting construct, an attacker having proper PostgreSQL privileges can execute arbitrary code in the system as the administrator.

CVSS v3.1 Base Score: 7.5 (High)
CVSS v3.1 Temporal Score: 7.5 (High)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE
CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-39417

CVE-2024-7348 Time-of-check Time-of-use

A 'time-of-check time-of-use' (TOCTOU) race condition in a PostgreSQL can allow an attacker to easily execute arbitrary SQL functions by leveraging a PostgreSQL utility often executed with high privileges.

[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.

CVSS v3.1 Base Score: 8.8 (High)
CVSS v3.1 Temporal Score: 8.8 (High)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE
CWE-367 - Time-of-check Time-of-use (TOCTOU) Race Condition.

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-7348

CVE-2024-0985 Late Privilege Drop in Materialized View

An attacker can provide untrusted materialized views and lure a high privileged authorized user to inadvertently execute arbitrary SQL functions by refreshing the attacker's materialized view.

CVSS v3.1 Base Score: 8.0 (High)
CVSS v3.1 Temporal Score: 8.0 (High)
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CWE
CWE-271 - Privilege Dropping / Lowering Errors.

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-0985

Mitigating factors

Any exploit of these vulnerabilities would require that the attacker has access to the site's S+ client/server network. Following ABB's recommended security practices, including network architecture and perimeter firewall, are mitigating factors in preventing external access to the S+ client/server network.

Refer to section "General security recommendations" 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 who successfully exploited these vulnerabilities could insert and run arbitrary code in the S+ system.

What causes the vulnerability?

It is caused by several vulnerabilities in the PostgreSQL version 13.11 and earlier versions component used by the S+ Engineering product (see Affected products).

What might an attacker use the vulnerability to do?

An attacker who successfully accessed the site's S+ client/server network could cause a denial-of-service situation, corruptions of data or unauthorized disclosure of information.

How could an attacker exploit the vulnerability?

To exploit the PostgreSQL vulnerabilities (see Vulnerability severity and details), an attacker should successfully access to the site's S+ client/server network, remotely (through a wrongly configured or penetrated firewall) or even compromising a local machine and then accessing to PostgreSQL.

Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, see the above How could an attacker exploit the 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 S+ Engineering update removes the vulnerability by installing a secure updated PostgreSQL version.

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

Yes, PostgreSQL 13.11 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 any information indicating that S+ Engineering 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:

<Document ID>	<Document title>
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
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	ABB ICS Cyber Security Reference Architecture - Document

References

7PAA014844D2421	S+ Engineering 2.4 SP2 Rollup 1 Release notes

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	04/10/2026