DOCUMENT ID: 7PAA006722
REVISION: A
DATE: 2023-02-15
SECURITY LEVEL: PUBLIC

CYBER SECURITY ADVISORY

SECURITY – Improper authentication vulnerability in S+ Operations

CVE ID: CVE-2023-0228

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

ABB Ability™ Symphony® Plus:

S+ Operations 3.3 SP2 (part of SPR[1] 2023.0)

S+ Operations 3.3 SP1 and earlier 3.x versions

S+ Operations 2.2

S+ Operations 2.1 SP2 and earlier 2.x versions

Vulnerability IDs

CVE-2023-0228

Summary

ABB has identified a vulnerability in the product versions listed above that could allow an unauthorized client to connect to the S+ Operations servers (HMI network), to act as a legitimate S+ Operations client.

An update for S+ Operations is being prepared but is not available yet. This document also describes some mitigations that can help concerned users limit their risk.   Note that this document may be updated if/when more information becomes available.

[1] System Package Release – a validated collection of Symphony Plus products released together.

Recommended immediate actions

ABB advises all customers to review their installations to determine if they are using an impacted product as listed above and follow below recommendations. No further analysis or tools are needed to make this determination.

End users should immediately apply the Mitigations listed below, as this will restrict or prevent an attacker's ability to compromise these systems.

S+ Operations 3.3 SP2 (part of SPR[2] 2023.0)
Follow the Mitigating Factors as described below and deploy the upcoming update for this version planned to be released within Q3 2023.

S+ Operations 3.3 SP1 and earlier 3.x versions
Follow the Mitigating Factors as described below and deploy the upcoming update for this version planned to be released within Q4 2023.

S+ Operations 2.2
Follow the Mitigating Factors as described below and deploy the upcoming update for this version planned to be released within Q4 2023.

S+ Operations 2.1 SP2 and earlier 2.x versions
Follow the Mitigating Factors as described below. Recommendation is to upgrade the system to version S+ Operations 3.3 with the updates described above to fully mitigate the issue.

Vulnerability severity and details

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[3].

CVE-2023-0228 Improper Authentication

An unauthorized client able to connect to the S+ Operations servers (HMI network) can act as a legitimate S+ Operations client, read any data and change its configuration, potentially resulting in corruption of data, unauthorized disclosure of information, unexpected operation of equipment or causing the product or the system to stop (denial of service).

CVSS v3.1 Base Score:	8.8 (High)
CVSS v3.1 Temporal Score:	7.8 (High)
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:W/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-0228

[2] System Package Release – a validated collection of Symphony Plus products released together.

[3] 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.

Mitigating factors

S+ Operations is not intended to be directly connected to the internet and is expected to follow the ABB's recommended approach of designing and deploying a secure network for industrial use (ICS Cyber Security Reference Architecture Guide, 8VZZ000368D0066).

An attack by an unauthorized client able to connect to the S+ Operations servers (HMI network) can be prevented by enabling host authentication and data integrity via IPsec (documented in “Symphony Plus Secure deployment guide for Windows 10 and Server 2016/2019 user manual”, 8VZZ001006T0001).

There are several security countermeasures at host-level that can be applied to mitigate the likelihood of an attack to the S+ Operations client machine, like Hardening practices and usage of malware prevention solutions (see section “What is the scope of the vulnerability?

An attacker able to connect to a S+ Operations server machine in the site’s HMI network (or if the machine gets locally compromised) could act as a legitimate S+ Operations client, potentially resulting in corruptions of data, unauthorized disclosure of information or causing the product or the system not to work properly.

What causes the vulnerability?

The vulnerability is caused by improper authentication at the client machine process level.

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 able to connect to a S+ Operations server in the site’s HMI network, and having a deep knowledge of S+ Operations internals, could corrupt data, disclose information, or cause S+ Operations (or the Symphony Plus system) to malfunction or even stop (denial of service).

How could an attacker exploit the vulnerability?

An attacker able to connect to a S+ Operations server in the site’s HMI network, and having a deep knowledge of S+ Operations internals, could exploit this vulnerability.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to a S+ Operations server in the site’s HMI network 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. Additionally, this vulnerability can be exploited by having local access to a S+ Operations server from within the site’s HMI network.

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?

Updates are being prepared to improve the authentication methodology to resolve this vulnerability.

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

No, this vulnerability has not 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 this vulnerability had been exploited when this security advisory was originally issued.

General security recommendations" for details).

If not properly secured and checked, removable media can represent a vector of attack. Whenever possible, it should be ensured that no removable media can be used at the site's HMI network or allowed for a short period of time as necessary (see ABB Security Policies about such media in "System 800xA, Symphony Plus and Freelance - System Hardening - End user manual", 2PAA122516).

Refer to section "What is the scope of the vulnerability?

An attacker able to connect to a S+ Operations server machine in the site's HMI network (or if the machine gets locally compromised) could act as a legitimate S+ Operations client, potentially resulting in corruptions of data, unauthorized disclosure of information or causing the product or the system not to work properly.

What causes the vulnerability?

The vulnerability is caused by improper authentication at the client machine process level.

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 able to connect to a S+ Operations server in the site's HMI network, and having a deep knowledge of S+ Operations internals, could corrupt data, disclose information, or cause S+ Operations (or the Symphony Plus system) to malfunction or even stop (denial of service).

How could an attacker exploit the vulnerability?

An attacker able to connect to a S+ Operations server in the site's HMI network, and having a deep knowledge of S+ Operations internals, could exploit this vulnerability.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to a S+ Operations server in the site's HMI network 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. Additionally, this vulnerability can be exploited by having local access to a S+ Operations server from within the site's HMI network.

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?

Updates are being prepared to improve the authentication methodology to resolve this vulnerability.

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

No, this vulnerability has not 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 this vulnerability had been exploited when this security advisory was originally issued.

General security recommendations" for further advice on how to keep your system secure.

Frequently asked questions

What is the scope of the vulnerability?

An attacker able to connect to a S+ Operations server machine in the site's HMI network (or if the machine gets locally compromised) could act as a legitimate S+ Operations client, potentially resulting in corruptions of data, unauthorized disclosure of information or causing the product or the system not to work properly.

What causes the vulnerability?

The vulnerability is caused by improper authentication at the client machine process level.

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 able to connect to a S+ Operations server in the site's HMI network, and having a deep knowledge of S+ Operations internals, could corrupt data, disclose information, or cause S+ Operations (or the Symphony Plus system) to malfunction or even stop (denial of service).

How could an attacker exploit the vulnerability?

An attacker able to connect to a S+ Operations server in the site's HMI network, and having a deep knowledge of S+ Operations internals, could exploit this vulnerability.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to a S+ Operations server in the site's HMI network 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. Additionally, this vulnerability can be exploited by having local access to a S+ Operations server from within the site's HMI network.

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?

Updates are being prepared to improve the authentication methodology to resolve this vulnerability.

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

No, this vulnerability has not 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 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[4]:

8VZZ001006T0001	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	Symphony Plus Security Updates Validation Status
7PAA003784	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	ICS Cyber Security Reference Architecture Guide

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.

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

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2023-02-10 PAPCP/RD