DOCUMENT ID: 2PAA123980
REVISION: A
DATE: 2020-12-14

CYBERSECURITY ADVISORY

SECURITY Multiple Vulnerabilities in Symphony® Plus Operations

Vulnerability ID: CVE-2020-24673, CVE-2020-24674, CVE-2020-24675, CVE-2020-24676, CVE-2020-24677, CVE-2020-24678, CVE-2020-24679, CVE-2020-24680, CVE-24683

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 cybersecurity 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 cybersecurity.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating 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 ICS-CERT.

The resulting Cybersecurity 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 Cybersecurity 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 Cybersecurity Advisory is an example 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. See details below.

Affected products

ABB Ability™ Symphony® Plus:

- S+ Operations 1.1
- S+ Operations 2.0 (including all Service Packs)
- S+ Operations 2.1 Service Pack 1 (SP1) (for Melody & other Heritage systems)
- S+ Operations 2.1 Service Pack 2 (SP2)
- S+ Operations 3.0
- S+ Operations 3.1
- S+ Operations 3.2
- S+ Operations 3.3

Summary

ABB has identified vulnerabilities in the product versions listed above. An update is available that resolves these vulnerabilities.

An attacker who successfully exploited one or more of these vulnerabilities could cause abuse the product functionality in various ways as described in the sections below.

Recommended immediate actions

ABB advises all customers to review their installations to determine if they are using an impacted system as listed above, no further analysis or tools are needed to make this determination.

Users are advised to upgrade to the latest release of S+ Operations (Version 3.3 Service Pack 1) which addresses the announced vulnerabilities as well as other technical issues and enhancements.

For customers using a version of S+ Operations older than 3.x and who cannot move to the current major release, there will be three additional maintenance releases to address the vulnerabilities:

- S+ Operations 2.1 SP2 Rollup 2 (Harmony, SD and Freelance only planned release: Q4 2020)
- S+ Operations 2.2 (Melody and Procontrol P14 systems only planned release: Q1 2021)
- S+ Operations 2.2 Rollup 1 (for Procontrol P13 systems only planned release: Q3 2021)

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 an attacker's ability to compromise these systems.

Vulnerability severity

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

CVE-2020-24673 - SQL Injection

CVSS v3.1 Base Score:	9.8 (Critical)
CVSS v3.1 Temporal Score:	9.1 (Critical)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-24673

CVE-2020-24674 - Improper Authorization

CVSS v3.1 Base Score:	8.8 (High)
CVSS v3.1 Temporal Score:	8.4 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-24674

CVE-2020-24675 - Weak Authentication

CVSS v3.1 Base Score:	9.8 (Critical)
CVSS v3.1 Temporal Score:	9.6 (Critical)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:W/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:W/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-24675

CVE-2020-24676 - Insecure Windows Services

CVSS v3.1 Base Score:	7.8 (High)
CVSS v3.1 Temporal Score:	7.2 (High)
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-24676

CVE-2020-24677 - Web Application Security

CVSS v3.1 Base Score:	8.8 (High)
CVSS v3.1 Temporal Score:	8.4 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-24677

CVE-2020-24678 - Privilege Escalation

CVSS v3.1 Base Score:	8.8 (High)
CVSS v3.1 Temporal Score:	8.4 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-24678

CVE-2020-24679 - Denial of Service

CVSS v3.1 Base Score:	7.5 (High)
CVSS v3.1 Temporal Score:	6.7 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/AR:H/MAV:N/MA:L
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-24679

CVE-2020-24680 - Improper Credential Storage

CVSS v3.1 Base Score:	7.0 (High)
CVSS v3.1 Temporal Score:	7.0 (High)
CVSS v3.1 Vector:	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-24680

CVE-2020-24683 – Authentication Bypass

CVSS v3.1 Base Score:	9.8 (Critical)
CVSS v3.1 Temporal Score:	9.1 (Critical)
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
CVSS v3.1 Link:	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
NVD Summary:	https://nvd.nist.gov/vuln/detail/CVE-2020-24683

Vulnerability details

ABB is aware that S+ Operations contains several vulnerabilities which require user attention:

1. **CVE-2020-24673 - SQL Injection**
   A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. This can lead to a loss of confidentiality and data integrity or even affect the product behavior and its availability.
2. **CVE-2020-24674 - Improper Authorization**
   Not all S+ Operations commands correctly check user permission as expected. Authenticated but Unauthorized remote users could execute a Denial-of-Service (DoS) attack, execute arbitrary code, or obtain more privilege than intended on the machines.
3. **CVE-2020-24675 - Weak Authentication**
   It is possible that an unauthenticated user could inject values to the Operations history server or ultimately write values to the controlled process.
4. **CVE-2020-24676 - Insecure Windows Services**
   Some services can be vulnerable to privilege escalation attacks. An unprivileged (but authenticated) user could execute arbitrary code and result in privilege escalation, depending on the user that the service runs as.
5. **CVE-2020-24677 - Web Application Security**
   Vulnerabilities in the S+ Operations web applications can lead to a possible code execution and privilege escalation, redirect the user somewhere else or download unwanted data.
6. **CVE-2020-24678 - Privilege Escalation**
   An authenticated user might execute malicious code under the user context and take control of the system. S+ Operations database is affected by multiple vulnerabilities such as the possibility to allow remote authenticated users to gain high privileges.
7. **CVE-2020-24679 - Denial of Service**
   A S+ Operations service is subject to a DoS by special crafted messages. An attacker might use this flaw to make it crash or even execute arbitrary code on the machine where the service is hosted.
8. **CVE-2020-24680 - Improper Credential Storage**
   The passwords of internal users (not Windows Users) are encrypted but improperly stored in a database.

9. **CVE-2020-24683 - Authentication Bypass**
   The affected versions of S+ Operations (version 2.1 SP1 and earlier) used an approach for user authentication which relies on validation at the client node (client-side authentication). This is not as secure as having the server validate a client application before allowing a connection. Therefore, if the network communication or endpoints for these applications are not protected, unauthorized actors can bypass authentication and make unauthorized connections to the server application.

Mitigating factors

The vulnerabilities announced in this Advisory for S+ Operations require that an attacker has access to the system network and hosts which are generally expected to be protected.

S+ Operations is NOT recommended to be exposed directly to Internet connections. If S+ Operation is placed into a DMZ which is not properly configured, then S+ Operations Web Applications may be remotely exploitable via some the vulnerabilities contained in this advisory.

To reduce the attack surface an important mitigation is to restrict network access. Methods for preventing unauthorized access to nodes on the system include but are not limited to the usage of IPsec (see "8VZZ001006T0001 - Symphony Plus Secure deployment guide for Windows 10 and Server 2016/2019") and by separating the S+ Operations client-server network from other networks with firewalls.

Another mitigation against attack is to ensure that only authorized persons have access to user accounts on the system nodes and proper protections against malicious code (like antivirus, security patches, recommended settings in "8VZZ001006T0001 - Symphony Plus Secure deployment guide for Windows 10 and Server 2016/2019" are applied and periodically updated. This also includes any user accounts accessing the system via remote tools like Remote Desktop.

Workarounds

Isolate S+ Operations network and Control System Domain from all external network connections.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploits the vulnerabilities listed may be able to modify plant operation data, alter reports and possibly send operating commands to the control system. Additionally, with escalated privileges the attacker could use the node to run arbitrary code and launch lateral attacks on other plant control system nodes.

What causes the vulnerability?

The listed vulnerabilities are caused by unchecked buffer size or input data, improper storage of sensitive data or incorrect implementation of the authentication/authorization mechanism and more. See section "Vulnerability details" above.

What is the affected product?

All previous releases of S+ Operations (version 3.3 and earlier).

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could prevent legitimate access to an affected system node, leading to a loss of its availability, or remotely cause an affected system node to stop. An attacker could also take control of the system, insert and run arbitrary code in a system node, gain higher privileges and obtain unauthorized access, leading to a loss of data confidentiality and integrity.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerabilities by creating a specially crafted message to the S+ Operations services or SQL database, executing arbitrary code, stealing sensitive data or gaining higher privileges. 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, S+ Operations Web Applications could expose functionality outside the local control system network. Further, some of the listed vulnerabilities can allow a remote authenticated attacker who has network access to escalate privileges, gain unauthorized access, and then use that to attempt lateral propagation to other control system nodes. 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.

What does the update do?

The update removes the above listed vulnerabilities by modifying the way how Symphony Plus Operations validates messages, authenticates users, verifies input data, and checks permissions.

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

No, ABB identified these vulnerabilities through internal testing and reviews.

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.

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 cybersecurity program and capabilities can be found at www.abb.com/cybersecurity.

Revisions

Rev.	Page (P) Chapt. (C)	Description	Date
A	all	New document	2020-12-14