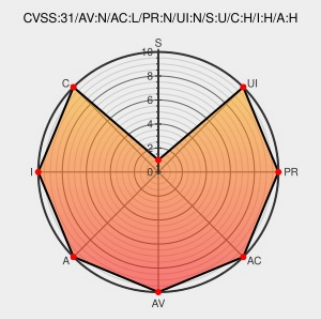
CVE-2020-24683

Published on: 12/22/2020 12:00:00 AM UTC

Last Modified on: 10/07/2021 07:05:00 PM UTC

CVE-2020-24683 - advisory for 2PAA123980, 2PAA123982

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Symphony Plus Historian from Abb contain the following vulnerability:

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.

CVE-2020-24683 has been assigned by cybersecurity@ch.abb.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **ABB** - **ABB Ability™ Symphony® Plus Operations** version **< 2.1 SP1**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	Mitigation Vendor Advisory search.abb.com application/pdf	MISC search.abb.com/library/Download.aspx?DocumentID=2PAA123980&LanguageCode=en&DocumentPartId=&Action=Launch

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Abb	Symphony Plus Historian	3.0	All	All	All
Application	Abb	Symphony Plus Historian	3.1	All	All	All
Application	Abb	Symphony Plus Historian	3.0	All	All	All
Application	Abb	Symphony Plus Historian	3.1	All	All	All
Application	Abb	Symphony Plus Operations	1.1	All	All	All
Application	Abb	Symphony Plus Operations	2.0	All	All	All
Application	Abb	Symphony Plus Operations	2.1	sp1	All	All
Application	Abb	Symphony Plus Operations	2.1	sp2	All	All
Application	Abb	Symphony Plus Operations	3.0	All	All	All
Application	Abb	Symphony Plus Operations	3.1	All	All	All
Application	Abb	Symphony Plus Operations	3.2	All	All	All
Application	Abb	Symphony Plus Operations	3.3	All	All	All
Application	Abb	Symphony Plus Operations	1.1	All	All	All
Application	Abb	Symphony Plus Operations	2.0	All	All	All
Application	Abb	Symphony Plus Operations	2.1	sp1	All	All
Application	Abb	Symphony Plus Operations	2.1	sp2	All	All
Application	Abb	Symphony Plus Operations	3.0	All	All	All
Application	Abb	Symphony Plus Operations	3.1	All	All	All
Application	Abb	Symphony Plus Operations	3.2	All	All	All
Application	Abb	Symphony Plus Operations	3.3	All	All	All
Application	Abb	Symphony Historian	3.0	All	All	All
Application	Abb	Symphony Historian	3.1	All	All	All
Application	Abb	Symphony Operations	1.1	All	All	All
Application	Abb	Symphony Operations	2.0	All	All	All

Application	Abb	Symphony Operations	2.1	sp1	All	All
Application	Abb	Symphony Operations	2.1	sp2	All	All
Application	Abb	Symphony Operations	3.0	All	All	All
Application	Abb	Symphony Operations	3.1	All	All	All
Application	Abb	Symphony Operations	3.2	All	All	All
Application	Abb	Symphony Operations	3.3	All	All	All

cpe:2.3:a:abb:symphony_plus_historian:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_historian:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_historian:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_historian:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:2.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:2.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:3.2:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:3.3:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:2.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:2.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:3.2:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_plus_operations:3.3:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_historian:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_historian:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_operations:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_operations:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_operations:2.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_operations:2.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_operations:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_operations:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_operations:3.2:*:*:*:*:*:*:*:

cpe:2.3:a:abb:symphony_\+_operations:3.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→