



CVE-2020-24675

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

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

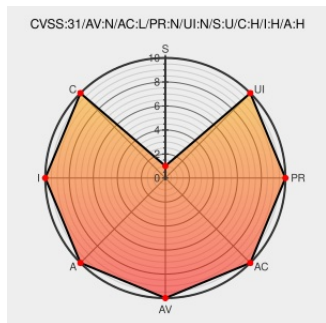
CVE-2020-24675 - advisory for 2PAA123980, 2PAA123982

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Symphony Plus Historian](#) from [Abb](#) contain the following vulnerability:

In S+ Operations and S+ History, it is possible that an unauthenticated user could inject values to the Operations History server (or standalone S+ History server) and ultimately write values to the controlled process.

CVE-2020-24675 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 < 3.3 Service Pack 1

Affected Vendor/Software: [ABB](#) - **ABB Ability™ Symphony® Plus Operations** version < 2.1 SP2 Rollup 2

Affected Vendor/Software: [ABB](#) - **ABB Ability™ Symphony® Plus Operations** version < 2.2

Affected Vendor/Software: [ABB](#) - **ABB Ability™ Symphony® Plus Historian** version < 3.2

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
SECURITY Multiple Vulnerabilities in S+ Historian	Mitigation	ABB MISC search.abb.com/library/Download.aspx?DocumentID=2PAA123982&LanguageCode=en&DocumentPartId=&Action=Launch
	Vendor Advisory search.abb.com text/html	
	Mitigation	ABB MISC search.abb.com/library/Download.aspx?DocumentID=2PAA123980&LanguageCode=en&DocumentPartId=&Action=Launch
	Vendor Advisory search.abb.com application/pdf	
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

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_plus_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→		