



CVE-2020-24676

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

Last Modified on: 09/14/2021 03:23:00 PM UTC

CVE-2020-24676 - advisory for 2PAA123980, 2PAA123982

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

In Symphony Plus Operations and Symphony Plus Historian, 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.

CVE-2020-24676 has been assigned by [cybersecurity@ch.abb.com](#) to track the vulnerability - currently rated as **HIGH** 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: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SECURITY Multiple Vulnerabilities in S+ Historian	Mitigation	 MISC search.abb.com/library/Download.aspx?DocumentID=2PAA123982&LanguageCode=en&DocumentPartId=&Action=Launch
	Vendor Advisory search.abb.com text/html	
	Mitigation	 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 Historian	3.0	All	All	All
Application	Abb	Symphony Historian	3.1	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
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_\+_historian:3.0:*:*:*:*:*:						
cpe:2.3:a:abb:symphony_\+_historian:3.1:*:*:*:*:*:						
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:*:*:*:*:*:						
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)
🔒 @LinInfoSec	Symphony - CVE-2020-24676: search.abb.com/library/Downlo...	2021-09-14 16:46:51

[← Previous ID](#)

Next ID→

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)