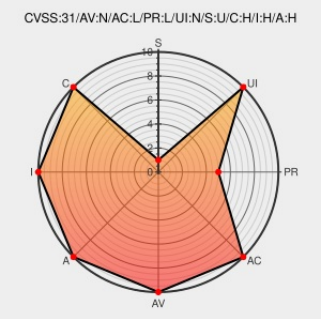
CVE-2022-3158

Published on: Not Yet Published

Last Modified on: 10/20/2022 02:42:00 PM UTC

CVE-2022-3158

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



Certain versions of Factorytalk Vantagepoint from Rockwellautomation contain the following vulnerability:

Rockwell Automation FactoryTalk VantagePoint versions 8.0, 8.10, 8.20, 8.30, 8.31 are vulnerable to an input validation vulnerability. The FactoryTalk VantagePoint SQL Server lacks input validation when users enter SQL statements to retrieve information from the back-end database. If successfully exploited, this could allow a user with basic user privileges to perform remote code execution on the server.

CVE-2022-3158 has been assigned by PSIRT@rockwellautomation.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
Factory Talk VantagePoint Software Broken Access Control and Input Validation Vulnerability	rockwellautomation.custhelp.com text/html	MISC rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137043

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	Rockwellautomation	Factorytalk Vantagepoint	8.0	All	All	All
Application	Rockwellautomation	Factorytalk Vantagepoint	8.10	All	All	All
Application	Rockwellautomation	Factorytalk Vantagepoint	8.20	All	All	All
Application	Rockwellautomation	Factorytalk Vantagepoint	8.30	All	All	All
Application	Rockwellautomation	Factorytalk Vantagepoint	8.31	All	All	All

cpe:2.3:a:rockwellautomation:factorytalk_vantagepoint:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:rockwellautomation:factorytalk_vantagepoint:8.10:*:*:*:*:*:*:*:

cpe:2.3:a:rockwellautomation:factorytalk_vantagepoint:8.20:*:*:*:*:*:*:*:

cpe:2.3:a:rockwellautomation:factorytalk_vantagepoint:8.30:*:*:*:*:*:*:*:

cpe:2.3:a:rockwellautomation:factorytalk_vantagepoint:8.31:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-3158	2022-10-17 23:38:12

← Previous ID

Next ID→