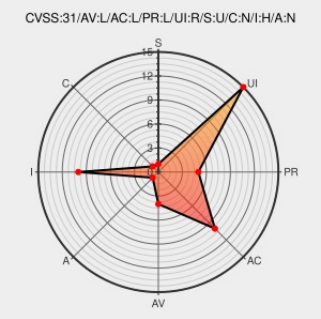
CVE-2023-2638

Published on: Not Yet Published

Last Modified on: 06/26/2023 04:28:00 PM UTC

CVE-2023-2638

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



Certain versions of Factorytalk Policy Manager from Rockwellautomation contain the following vulnerability:

Rockwell Automation's FactoryTalk System Services does not verify that a backup configuration archive is password protected. Improper authorization in FTSSBackupRestore.exe may lead to the loading of malicious configuration archives. This vulnerability may allow a local, authenticated non-admin user to craft a malicious backup archive, without password protection, that will be loaded by FactoryTalk System Services as a valid backup when a restore procedure takes places. User interaction is required for this vulnerability to be successfully exploited.

CVE-2023-2638 has been assigned by PSIRT@rockwellautomation.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Rockwell Automation** - **FactoryTalk System Services** version **= <= 6.20**

CVSS3 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
FactoryTalk® System Services affecting FactoryTalk® Policy Manager – Multiple Vulnerabilities	rockwellautomation.custhelp.com text/html	MISC rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139683

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 Policy Manager	6.11.0	All	All	All
Application	Rockwellautomation	Factorytalk System Services	6.11.0	All	All	All

cpe:2.3:a:rockwellautomation:factorytalk_policy_manager:6.11.0:*:*:*:*:*:*:*:

cpe:2.3:a:rockwellautomation:factorytalk_system_services:6.11.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→