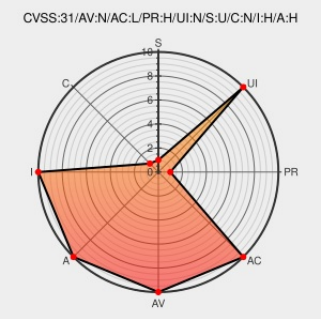
CVE-2022-47917

Published on: Not Yet Published

Last Modified on: 01/26/2023 01:43:00 PM UTC

CVE-2022-47917

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



Certain versions of Real-time Location System Studio from Sewio contain the following vulnerability:

Sewio's Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 is vulnerable to improper input validation of user input to several modules and services of the software. This could allow an attacker to delete arbitrary files and cause a denial-of-service condition.

CVE-2022-47917 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Sewio** - **RTLS Studio** version **= 2.0.0**

Vulnerability Patch/Work Around

Sewio also recommends the following workarounds to reduce the risk of exploitation: * Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the internet https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-10-301-01 . * Locate control system networks and remote devices behind firewalls and isolate them from business networks.

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
Sewio RTLS Studio | CISA	www.cisa.gov text/html	MISC www.cisa.gov/uscert/ics/advisories/icsa-23-012-01

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

Exploit/POC from Github

Sewio's Real-Time Location System (RTLS) Studio version 2.0.0 up to and including version 2.6.2 is vulnerable to impr…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sewio	Real-time Location System Studio	All	All	All	All

cpe:2.3:a:sewio:real-time_location_system_studio:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-47917	2023-01-18 02:38:34

← Previous ID

Next ID→