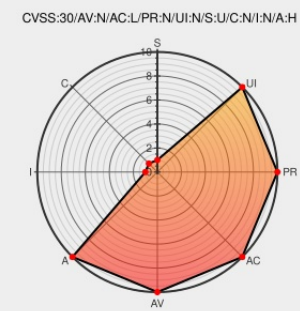
CVE-2017-1000230

Published on: 11/17/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:36 PM UTC

CVE-2017-1000230

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



Certain versions of Snap7 Server from Snap7 Project contain the following vulnerability:

The Snap7 Server version 1.4.1 can be crashed when the ItemCount field of the ReadVar or WriteVar functions of the S7 protocol implementation in Snap7 are provided with unexpected input, thus resulting in denial of service attack.

CVE-2017-1000230 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Snap7 / Discussion / Bugs reporting: Snap7 Server crashes when provided with unexpected input	Third Party Advisory, sourceforge.net, text/html	MISC sourceforge.net/p/snap7/discussion/bugfix/thread/2d2d085c/

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	Snap7 Project	Snap7 Server	1.4.1	All	All	All
Application	Snap7 Project	Snap7 Server	1.4.1	All	All	All

cpe:2.3:a:snap7_project:snap7_server:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:snap7_project:snap7_server:1.4.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→