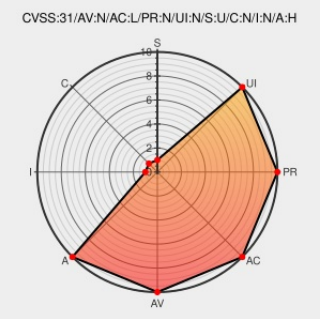
CVE-2020-22552

Published on: 10/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:10 PM UTC

CVE-2020-22552

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



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

The Snap7 server component in version 1.4.1, when an attacker sends a crafted packet with COTP protocol the last-data-unit flag set to No and S7 writes a var function, the Snap7 server will be crashed.

CVE-2020-22552 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.com - This website is for sale! - mobile app stock Resources and Information.	Third Party Advisory snap7.com text/html	MISC snap7.com
Snap7 / Discussion / Bugs reporting: SNAP7 will	Third Party Advisory	MISC

crash when Func Write and COTP last-data-unit flag is No	sourceforge.net text/html	sourceforge.net/p/snap7/discussion/bugfix/thread/456d76fdde/
Snap7 | Free Communications software downloads at SourceForge.net	Exploit Third Party Advisory sourceforge.net text/html	MISC sourceforge.net/projects/snap7/

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

cpe:2.3:a:snap7_project:snap7:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:snap7_project:snap7:1.4.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→