



# CVE-2021-33882

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-33882
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-25 12:15:00 UTC
<b>Updated</b>	2021-09-01 15:52:00 UTC
<b>Description</b>	A Missing Authentication for Critical Function vulnerability in B. Braun SpaceCom2 prior to 012U000062 allows a remote att

## Risk And Classification

**Problem Types:** CWE-306

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Bbraun	Infusomat Large Volume Pump 871305u	-	All	All	All
Operating System	Bbraun	Spacecom2	All	All	All	All
Hardware	Bbraun	Spacestation 8713142u	-	All	All	All

## References

Reference	Source	Link
404 Not Found	MISC	<a href="http://www.bbraunusa.com">www.bbraunusa.com</a>
McAfee Enterprise ATR Uncovers Vulnerabilities in Globally Used B. Braun Infusion Pump   McAfee Blogs	MISC	<a href="http://www.mcafee.com">www.mcafee.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)