



CVE-2021-20832

Published on: 10/13/2021 12:00:00 AM UTC

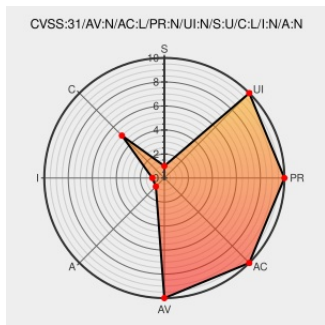
Last Modified on: 10/19/2021 01:53:00 PM UTC

CVE-2021-20832

Source: Mitre

Source: Nist

Print: PDF



Certain versions of **Inbody** from **Inbody** contain the following vulnerability:

InBody App for iOS versions prior to 2.3.30 and InBody App for Android versions prior to 2.2.90(510) contain a vulnerability which may lead to information disclosure only when it works with the body composition analyzer InBody Dial. This may allow an attacker who can connect to the InBody Dial with InBody App may obtain a victim's measurement result measured by InBody Dial.

CVE-2021-20832 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **InBody Japan Inc. - InBody App for iOS versions prior to 2.3.30 and InBody App for Android versions prior to 2.2.90(510)** version **InBody App for iOS versions prior to 2.3.30 and InBody App for Android versions prior to 2.2.90(510)**

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
JVN#63023305: InBody App vulnerable to information disclosure	jvn.jp text/xml	MISC jvn.jp/en/jp/JVN63023305/index.html
InBody Dial セキュリティ強化のためのアプリアップデートのご案内 – 【公式】体成分分析装置InBody インボディ	www.inbody.co.jp text/html	MISC www.inbody.co.jp/inbody-news/?uid=55&mod=document&pageid=1

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	Inbody	Inbody	All	All	All	All
Application	Inbody	Inbody	All	All	All	All

`cpe:2.3:a:inbody:inbody:*:*:*:*:android:*:*:`

`cpe:2.3:a:inbody:inbody:*:*:*:*:iphone_os:*:*:`

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-20832 : InBody App for iOS versions prior to 2.3.30 and InBody App for Android versions prior to 2.2.90 51... twitter.com/i/web/status/1...	2021-10-13 08:41:28
@WesUncensored	New vulnerability on the NVD: CVE-2021-20832 ift.tt/3iXP19v	2021-10-13 10:33:29
@workentin	New vulnerability on the NVD: CVE-2021-20832 ift.tt/3iXP19v	2021-10-13 10:40:11

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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