

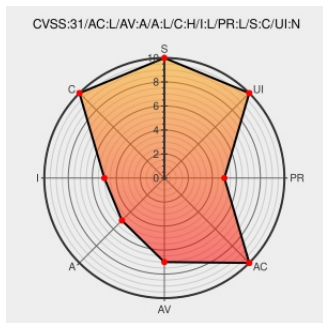


CVE-2022-30904

Published on: Not Yet Published

Last Modified on: 02/09/2023 07:47:00 PM UTC

CVE-2022-30904

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Bes2300](#) from [Bestechnic](#) contain the following vulnerability:

In Bestechnic Bluetooth Mesh SDK (BES2300) V1.0, a buffer overflow vulnerability can be triggered during provisioning, because there is no check for the SegN field of the Transaction Start PDU.

CVE-2022-30904 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
CVE-2022-30904.docx - Google Docs	docs.google.com text/html	G MISC docs.google.com/document/d/1is3dYwMcRlkhjvujzi5OgnaGBsQVtlew/edit

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](#)

In Bestechnic Bluetooth Mesh SDK (BES2300) V1.0, a buffer overflow vulnerability can be

In Bestechnic Bluetooth Mesh SDK (BES2300) V1.0, a buffer overflow vulnerability can be triggered during provisioning...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Bestechnic	Bes2300	-	All	All	All
Application	Bestechnic	Bluetooth Mesh Software Development Kit	1.0	All	All	All
cpe:2.3:h:bestechnic:bes2300:-:*:*:*:*:*:						
cpe:2.3:a:bestechnic:bluetooth_mesh_software_development_kit:1.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-30904 : In Bestechnic Bluetooth Mesh SDK BES2300 V1.0, a buffer overflow vulnerability can be triggered... twitter.com/i/web/status/1...	2023-02-01 21:05:11
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-30904 In Bestechnic Bluetooth Mesh SDK (BES2300) V1.0, a buffer overflo... twitter.com/i/web/status/1...	2023-02-01 21:56:00
 /r/netcve	CVE-2022-30904	2023-02-01 21:40:35

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2023   |

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](#)