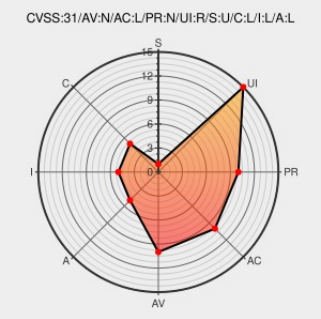
CVE-2022-3785

Published on: Not Yet Published

Last Modified on: 11/03/2022 04:42:00 PM UTC

CVE-2022-3785

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



Certain versions of Bento4 from Axiosys contain the following vulnerability:

A vulnerability, which was classified as critical, has been found in Axiomatic Bento4. Affected by this issue is the function AP4_DataBuffer::SetDataSize of the component Avcinfo. The manipulation leads to heap-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212564.

CVE-2022-3785 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Axiomatic** - **Bento4** version **n/a**

CVSS3 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
	github.com application/zip	MISC github.com/axiomatic-systems/Bento4/files/9658653/POC_avcinfo_15644345.zip
A heap-buffer-overflow in Avcinfo · Issue #780 · axiomatic-systems/Bento4 · GitHub	github.com text/html	MISC github.com/axiomatic-systems/Bento4/issues/780
CVE-2022-3785 | Axiomatic Bento4 Avcinfo SetDataSize heap-based overflow	vuldb.com text/html	MISC vuldb.com/?id.212564

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	Axiosys	Bento4	1.6.0-639	All	All	All

cpe:2.3:a:axiosys:bento4:1.6.0-639:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-3785	2022-10-31 22:38:40

← Previous ID

Next ID→