

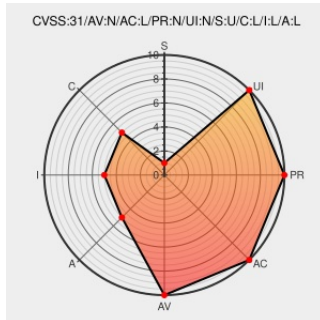


CVE-2022-3664

Published on: Not Yet Published

Last Modified on: 10/28/2022 05:29:00 PM UTC

CVE-2022-3664

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

Certain versions of [Bento4](#) from [Axiosys](#) contain the following vulnerability:

A vulnerability classified as critical has been found in Axiomatic Bento4. Affected is the function `AP4_BitStream::WriteBytes` of the file `Ap4BitStream.cpp` of the component `avcinfo`. The manipulation leads to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-212004.

CVE-2022-3664 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/9746288/avcinfo_poc1.zip
CVE-2022-3664 Axiomatic Bento4 avcinfo Ap4BitStream.cpp WriteBytes heap-based overflow (ID 794)	web.archive.org text/html Inactive Link Not Archived	MISC vuldb.com/?id.212004
Some heap buffer overflow bugs exist in avcinfo · Issue #794 · axiomatic-systems/Bento4 · GitHub	github.com text/html	MISC github.com/axiomatic-systems/Bento4/issues/794

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

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

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-2022-3664	2022-10-26 18:38:30

[← 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](#)