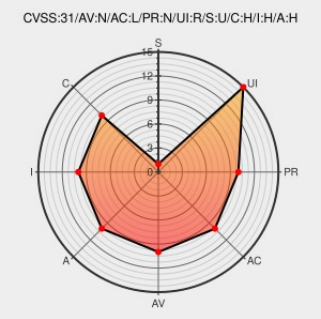
CVE-2022-4584

Published on: Not Yet Published

Last Modified on: 10/20/2023 03:09:32 PM UTC

CVE-2022-4584

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



Certain versions of Bento4 from Axiosys contain the following vulnerability:

A vulnerability was found in Axiomatic Bento4 up to 1.6.0-639. It has been rated as critical. Affected by this issue is some unknown functionality of the component mp42aac. 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. VDB-216170 is the identifier assigned to this vulnerability.

CVE-2022-4584 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Axiomatic** - **Bento4** version **= 1.6.0-639**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
CVE-2022-4584 | Axiomatic Bento4 mp42aac heap-based overflow (ID 818)	vuldb.com text/html	MISC vuldb.com/?id.216170
heap-buffer-overflow in mp42aac · Issue #818 · axiomatic-systems/Bento4 · GitHub	github.com text/html	MISC github.com/axiomatic-systems/Bento4/issues/818
	github.com application/gzip	MISC github.com/axiomatic-systems/Bento4/files/10095915/POC2.tar.gz
	vuldb.com text/plain	MISC vuldb.com/?ctiid.216170

Inactive Link | Not Archived

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	-	All	All	All
Application	Axiosys	Bento4	All	All	All	All

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

cpe:2.3:a:axiosys:bento4:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-4584 : A vulnerability was found in Axiomatic Bento4. It has been rated as critical. Affected by this issu… twitter.com/i/web/status/1…	2022-12-17 13:14:42
/r/netcve	CVE-2022-4584	2022-12-17 13:39:10

← Previous ID

Next ID→