CVE-2022-3974

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-3974
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-13 10:15:00 UTC
Updated	2023-11-07 03:52:00 UTC
Description	A vulnerability classified as critical was found in Axiomatic Bento4. Affected by this vulnerability is the function AP4_StdcFil

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Axiosys	Bento4	2022-10-08	All	All	All

References

Reference	Source	Li
N/A	N/A	git
CVE-2022-3974 | Axiomatic Bento4 mp4info Ap4StdCFileByteStream.cpp ReadPartial heap-based overflow	N/A	vu
Heap overflow in mp4info, ReadPartial, Ap4StdCFileByteStream.cpp:341 · Issue #812 · axiomatic-systems/Bento4 · GitHub	N/A	git
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report