



CVE-2017-14638

Published on: 09/21/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:45 PM UTC

CVE-2017-14638

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

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

AP4_AtomFactory::CreateAtomFromStream in Core/Ap4AtomFactory.cpp in Bento4 version 1.5.0-617 has missing NULL checks, leading to a NULL pointer dereference, segmentation fault, and application crash in AP4_Atom::SetType in Core/Ap4Atom.h.

CVE-2017-14638 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
NULL pointer dereference in AP4_Atom::SetType (Ap4Atom.h) · Issue #182 · axiomatic-systems/Bento4 · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/axiomatic-systems/Bento4/issues/182

bento4: NULL pointer dereference in AP4_Atom::SetType (Ap4Atom.h) | agostino's blog

Exploit

Issue Tracking

Patch

Third Party Advisory

VDB Entry

blogs.gentoo.org

text/html

MISC blogs.gentoo.org/ago/2017/09/14/bento4-null-pointer-dereference-in-ap4_atomsettype-ap4atom-h/

fix for #182 · axiomatic-systems/Bento4@be7185f · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC github.com/axiomatic-systems/Bento4/commit/be7185faf7f52674028977dcf501c6039ff03aa5

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	Bento4	Bento4	1.5.0-617	All	All	All
Application	Bento4	Bento4	1.5.0-617	All	All	All
cpe:2.3:a:bento4:bento4:1.5.0-617:****:***:						
cpe:2.3:a:bento4:bento4:1.5.0-617:****:***:						

No vendor comments have been submitted for this CVE