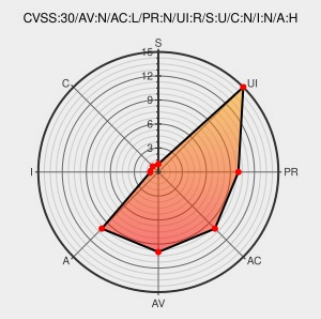
CVE-2017-14643

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

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

CVE-2017-14643

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



Certain versions of Bento4 from Bento4 contain the following vulnerability:

The AP4_HdlrAtom class in Core/Ap4HdlrAtom.cpp in Bento4 version 1.5.0-617 uses an incorrect character data type, leading to a heap-based buffer over-read and application crash in AP4_BytesToUInt32BE in Core/Ap4Utils.h.

CVE-2017-14643 has been assigned by 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
fix for #187 · axiomatic-systems/Bento4@5eb8cf8 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/axiomatic-systems/Bento4/commit/5eb8cf89d724ccb0b4ce5f24171ec7c11f0a7647

heap-based buffer overflow in AP4_BytesToUInt32BE (Ap4Utils.h) · Issue #187 · axiomatic-systems/Bento4 · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/axiomatic-systems/Bento4/issues/187
bento4: heap-based buffer overflow in AP4_BytesToUInt32BE (Ap4Utils.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-heap-based-buffer-overflow-in-ap4_bytestouint32be-ap4utils-h/

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

← Previous ID

Next ID→