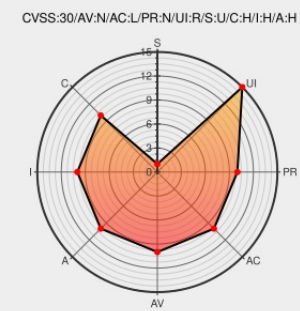
CVE-2017-14639

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

Last Modified on: 03/23/2021 11:26:44 PM UTC

CVE-2017-14639

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



Certain versions of Bento4 from Bento4 contain the following vulnerability:

AP4_VisualSampleEntry::ReadFields in Core/Ap4SampleEntry.cpp in Bento4 1.5.0-617 uses incorrect character data types, which causes a stack-based buffer underflow and out-of-bounds write, leading to denial of service (application crash) or possibly unspecified other impact.

CVE-2017-14639 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
fix for #190 · axiomatic-systems/Bento4@03d1222 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/axiomatic-systems/Bento4/commit/03d1222ab9c2ce779cdf01bdb96cdd69cbdcfeda

stack-based buffer underflow in AP4_VisualSampleEntry::ReadFields (Ap4SampleEntry.cpp) · Issue #190 · axiomatic-systems/Bento4 · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/axiomatic-systems/Bento4/issues/190
bento4: stack-based buffer underflow in AP4_VisualSampleEntry::ReadFields (Ap4SampleEntry.cpp) | 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-stack-based-buffer-underflow-in-ap4_visualsampleentryreadfields-ap4sampleentry-cpp/

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→