VDB-354387 · CVE-2026-5236 · ISSUE 1059

AXIOMATIC BENTO4 UP TO 1.6.0-641 DSI V1 PARSER AP4DAC4ATOM.CPP AP4_BITREADER::SKIPBITS N_PRESENTATIONS HEAP-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.8	$0-$5k	2.31

Summary

A vulnerability was found in Axiomatic Bento4 up to 1.6.0-641. It has been classified as critical. Affected by this vulnerability is the function `AP4_BitReader::SkipBits` of the file *Ap4Dac4Atom.cpp* of the component *DSI v1 Parser*. Performing a manipulation of the argument *n_presentations* results in heap-based overflow. This vulnerability is reported as CVE-2026-5236. The attack requires a local approach. Moreover, an exploit is present. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability, which was classified as critical, was found in Axiomatic Bento4 up to 1.6.0-641. This affects the function `AP4_BitReader::SkipBits` of the file *Ap4Dac4Atom.cpp* of the component *DSI v1 Parser*. The manipulation of the argument `n_presentations` with an unknown input leads to a heap-based overflow vulnerability. CWE is classifying the issue as CWE-122. A heap overflow condition is a buffer overflow, where the buffer that can be overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as malloc(). This is going to have an impact on confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is uniquely identified as CVE-2026-5236. The exploitability is told to be easy. Attacking locally is a requirement. Technical details and a public exploit are known.

The exploit is shared for download at github.com. It is declared as proof-of-concept. The project was informed of the problem early through an issue report but has not responded yet.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The entries VDB-112829, VDB-223734 and VDB-239216 are pretty similar.

Product

Type

- Multimedia Player Software

Vendor

- Axiomatic

Name

- Bento4

Version

- 1.6.0-641

License

- free

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 4.8

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Heap-based overflow
CWE: CWE-122 / CWE-119
CAPEC: 🔒
ATT&CK: 🔒

Physical: Partially
Local: Yes
Remote: No

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

03/31/2026		Advisory disclosed
03/31/2026	+0 days	VulDB entry created
03/31/2026	+0 days	VulDB entry last update

Sources

Advisory: 1059
Status: Not defined

CVE: CVE-2026-5236 (🔒)
GCVE (CVE): GCVE-0-2026-5236
GCVE (VulDB): GCVE-100-354387
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/31/2026 04:14 PM
Changes: 03/31/2026 04:14 PM (60)
Complete: 🔍
Submitter: breakingbad
Cache ID: 57:5C6:179

Submit

Accepted

- Submit #780473: Bento4 <=1.6.0-641 Memory Corruption (by breakingbad)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa