



Home > Submit > 780473

Submit #780473: Bento4 <=1.6.0-641 Memory Corruption

Title Bento4 <=1.6.0-641 Memory Corruption

Description A heap-buffer-overflow vulnerability was found in AP4_Dac4Atom DSI v1 parsing in Ap4Dac4Atom.cpp. A crafted MP4 file with a dac4 atom containing a large n_presentations value (up to 511) causes AP4_BitReader::SkipBits() to read far beyond the heap-allocated buffer. This leads to out-of-bounds read (CWE-125), causing potential information disclosure or denial of service.

Source <https://github.com/axiomatic-systems/Bento4/issues/1059>

User breakingbad (UID 96046)

Submission 03/15/2026 04:28 PM (16 days ago)

Moderation 03/31/2026 04:09 PM (16 days later)

Status Accepted

VulDB entry VulDB [Axiomatic Bento4 up to 1.6.0-641 DSI v1 Parser Ap4Dac4Atom.cpp AP4_BitReader::SkipBits n_presentations heap-based overflow]

Points 19

Community Content

Submissions are made by [VulDB community users](#). VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- [Submission Policy](#)
- [Data Processing](#)
- [CVE Handling](#)