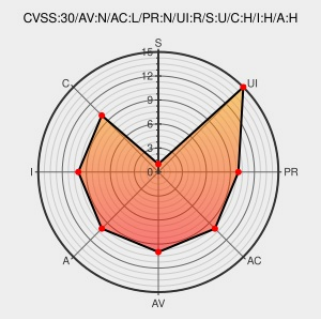
CVE-2019-8382

Published on: 02/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:56 PM UTC

CVE-2019-8382

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



Certain versions of Bento4 from Axiosys contain the following vulnerability:

An issue was discovered in Bento4 1.5.1-628. A NULL pointer dereference occurs in the function AP4_List:Find located in Core/Ap4List.h when called from Core/Ap4Movie.cpp. It can be triggered by sending a crafted file to the mp4dump binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact.

CVE-2019-8382 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
CVE-2019-8382: NULL POINTER DEREFERENCE Vulnerability in function AP4_List:Find() - Bento4-1.5.1-628 - Loginsoft	Exploit, Third Party Advisory	MISC research.loginsoft.com/bugs/null-pointer-dereference-vulnerability-in-function-

Research	research.loginsoft.com text/html	ap4_listfind-bento4-1-5-1-628/
NULL POINTER DEREFERENCE in AP4_List: Find () · Issue #364 · axiomatic-systems/Bento4 · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/axiomatic-systems/Bento4/issues/364

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Axiosys	Bento4	1.5.1-628	All	All	All
Application	Axiosys	Bento4	1.5.1-628	All	All	All

cpe:2.3:a:axiosys:bento4:1.5.1-628:*:*:*:*:*:*:*:

cpe:2.3:a:axiosys:bento4:1.5.1-628:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→