



CVE-2023-2961

Published on: Not Yet Published

Last Modified on: 06/21/2023 05:56:00 PM UTC

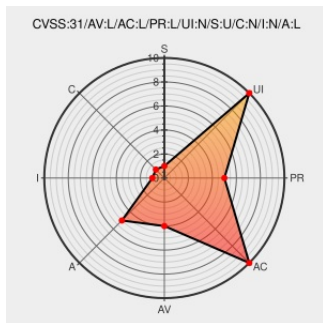
CVE-2023-2961

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Advancecomp](#) from [Advancemame](#) contain the following vulnerability:

A segmentation fault flaw was found in the Advancecomp package. This may lead to decreased availability.

CVE-2023-2961 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **LOW** severity.

CVSS3 Score: **3.3 - LOW**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

LOCAL

LOW

LOW

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

NONE

NONE

LOW

CVE References

Description

Tags

Link

2210768 – (CVE-2023-2961) CVE-2023-2961 advancecomp: SEGV via invalid read address

bugzilla.redhat.com
text/html

MISC
bugzilla.redhat.com/show_bug.cgi?id=2210768

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[182325](#) Debian Security Update for advancecomp (CVE-2023-2961)

[907310](#) Common Base Linux Mariner (CBL-Mariner) Security Update for advancecomp (27187-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Advancemame	Advancecomp	All	All	All	All
cpe:2.3:a:advancemame:advancecomp:*.*.*.*.*.*.*.*.						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report