



CVE-2023-26266

Published on: Not Yet Published

Last Modified on: 03/02/2023 11:03:00 PM UTC

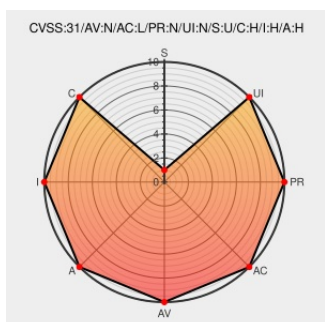
CVE-2023-26266

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Afl](#) from [Afl Project](#) contain the following vulnerability:

In AFL++ 4.05c, the CmpLog component uses the current working directory to resolve and execute unprefixed fuzzing targets, allowing code execution.

CVE-2023-26266 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Cmplog should search for unprefixed target in PATH, not PWD by YSaxon · Pull Request #1643 · AFLplusplus/AFLplusplus · GitHub	github.com text/html	MISC github.com/AFLplusplus/AFLplusplus/pull/1643

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

181921 Debian Security Update for aflplusplus (CVE-2023-26266)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Afl Project	Afl	4.05c	All	All	All
cpe:2.3:a:afl\+\+_project:afl\+\+:4.05c:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title					Posted (UTC)
 @CVEreport	CVE-2023-26266 : In AFL++ 4.05c, the CmpLog component uses the current working directory to resolve and execute unp... twitter.com/i/web/status/1...					2023-02-21 04:07:03
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-26266 In AFL++ 4.05c, the CmpLog component uses the current working dir... twitter.com/i/web/status/1...					2023-02-21 04:56:01
 /r/netcve	CVE-2023-26266					2023-02-21 05:38:21
← Previous ID			Next ID →			