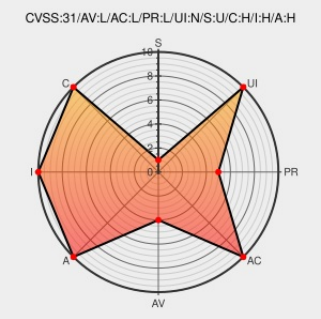
# CVE-2020-28840

Published on: Not Yet Published

Last Modified on: 08/21/2023 05:17:00 PM UTC

## CVE-2020-28840

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




Certain versions of Jhead from Matthiaswandel contain the following vulnerability:

Buffer Overflow vulnerability in jpgfile.c in Matthias-Wandel jhead version 3.04, allows local attackers to execute arbitrary code and cause a denial of service (DoS).

CVE-2020-28840 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 7.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| LOCAL | LOW | LOW | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVE References

| Description | Tags | Link |
|---|---|---|
| heap-buffer-overflow on process_COM in jpgfile.c:51 · Issue #8 · Matthias-Wandel/jhead · GitHub | github.com text/html | MISC github.com/Matthias-Wandel/jhead/issues/8 |
| A 'fix' to satisfy pednatic debian fuzzers. This one read ONE byte p… · Matthias-Wandel/jhead@4827ed3 · GitHub | github.com text/html | MISC github.com/Matthias-Wandel/jhead/commit/4827ed31c226dc5ed93603bd649e0e387a1778da |
| heap-buffer-overflow on process_COM in jpgfile.c:51 · Advisory · Fstark-prog/jhead · GitHub | github.com text/html | MISC github.com/F-ZhaoYang/jhead/security/advisories/GHSA-xh27-xwgj-gqw2 |
| Bug #1900820 “heap-buffer-overflow in jpgfile.c:51 process_COM” : Bugs : jhead package : Ubuntu | bugs.launchpad.net text/html | MISC bugs.launchpad.net/ubuntu/+source/jhead/+bug/1900820 |

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.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Matthiaswandel | Jhead | All | All | All | All |

cpe:2.3:a:matthiaswandel:jhead:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→



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