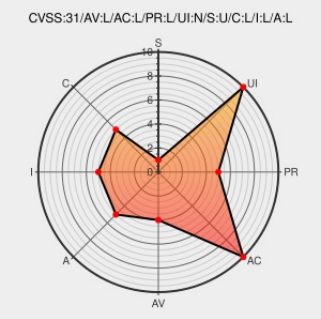
# CVE-2020-26208

Published on: 02/02/2022 12:00:00 AM UTC

Last Modified on: 02/07/2022 03:54:00 PM UTC

## **CVE-2020-26208** - advisory for GHSA-7pr6-xq4f-qhgc

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




Certain versions of Jhead from Jhead Project contain the following vulnerability:

JHEAD is a simple command line tool for displaying and some manipulation of EXIF header data embedded in Jpeg images from digital cameras. In affected versions there is a heap-buffer-overflow on jhead-3.04/jpgfile.c:285 ReadJpegSections. Crafted jpeg images can be provided to the user resulting in a program crash or potentially incorrect exif information retrieval. Users are advised to upgrade. There is no known workaround for this issue.

CVE-2020-26208 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 6.1 - MEDIUM

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

### CVSS2 Score: 5.8 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|

| | | |
|---|---|---|
| heap-buffer-overflow on jhead-3.04/jpgfile.c:285 ReadJpegSections · Advisory · F-ZhaoYang/jhead · GitHub | github.com text/html | CONFIRM github.com/F-ZhaoYang/jhead/security/advisories/GHSA-7pr6-xq4f-qhgc |
| heap-buffer-overflow on jhead-3.04/jpgfile.c:285 ReadJpegSections · Issue #7 · Matthias-Wandel/jhead · GitHub | github.com text/html | MISC github.com/Matthias-Wandel/jhead/issues/7 |
| Bug #1900821 “heap-buffer-overflow on jhead-3.04/jpgfile.c:285 R...” : Bugs : jhead package : Ubuntu | bugs.launchpad.net text/html | MISC bugs.launchpad.net/ubuntu/+source/jhead/+bug/1900821 |
| Just allocate 20 bytes extra at the end of a section. Otherwise, we end · F-ZhaoYang/jhead@5186ddc · GitHub | github.com text/html | MISC github.com/F-ZhaoYang/jhead/commit/5186ddcf9e35a7aa0ff0539489a930434a1325f4 |



## Related QID Numbers

180666 Debian Security Update for jhead (CVE-2020-26208)

199359 Ubuntu Security Notification for Jhead Vulnerabilities (USN-6098-1)

## Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:jhead_project:jhead:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| @CVEreport | CVE-2020-26208 : JHEAD is a simple command line tool for displaying and some manipulation of EXIF header data embed… twitter.com/i/web/status/1… | 2022-02-02 11:59:03 |
| /r/netcve | CVE-2020-26208 | 2022-02-02 13:38:45 |

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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