

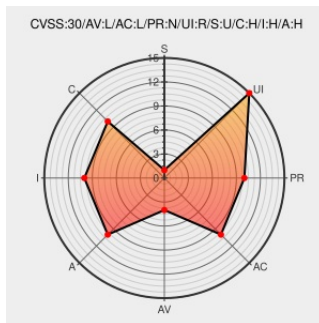


CVE-2018-16554

Published on: 09/15/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:33 PM UTC

CVE-2018-16554

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

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

The ProcessGpsInfo function of the gpsinfo.c file of jhead 3.00 may allow a remote attacker to cause a denial-of-service attack or unspecified other impact via a malicious JPEG file, because of inconsistency between float and double in a sprintf format string during TAG_GPS_ALT handling.

CVE-2018-16554 has been assigned by [M](#) 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	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
Page not found · GitHub Pages	Exploit Patch Third Party Advisory	MISC nimo-zhang.github.io/2018/09/07/bug-analysis-1/#more

nimo-zhang.github.io

text/html

Inactive Link

Not Archived

#908176 - jhead: CVE-2018-16554: Buffer overflow in gpsinfo.c while running jhead - Debian Bug report logs

Exploit

Mailing List

Third Party Advisory

bugs.debian.org

text/html

MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=908176

[SECURITY] [DLA 2054-1] jhead security update

lists.debian.org

text/html

MLIST [debian-lts-announce] 20191231 [SECURITY] [DLA 2054-1] jhead security update

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

750206 OpenSUSE Security Update for jhead (openSUSE-SU-2021:0743-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jhead Project	Jhead	3.00	All	All	All
Application	Jhead Project	Jhead	3.00	All	All	All

cpe:2.3:a:jhead_project:jhead:3.00:*****:

cpe:2.3:a:jhead_project:jhead:3.00:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →