



CVE-2020-6625

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-6625
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-09 01:15:00 UTC
Updated	2022-11-08 02:50:00 UTC
Description	jhead through 3.04 has a heap-based buffer over-read in Get32s when called from ProcessGpsInfo in gpsinfo.c.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
Bug #1858746 "heap-buffer-overflow on jhead-3.04/exif.c:336 Get3..." : Bugs : jhead package : Ubuntu	MISC
876247 – (CVE-2020-6624, CVE-2020-6625) media-gfx/jhead: multiple vulnerabilities	MISC
JHead: Multiple vulnerabilities (GLSA 202007-17) — Gentoo security	GENTOO
711220 – (CVE-2019-1010301, CVE-2019-1010302) <media-gfx/jhead-3.04: Multiple vulnerabilities (CVE-2019-{1010301,1010302})	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)