



CVE-2021-3496

Published on: 04/22/2021 12:00:00 AM UTC

Last Modified on: 12/21/2022 03:01:00 PM UTC

CVE-2021-3496

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

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

A heap-based buffer overflow was found in jhead in version 3.06 in Get16u() in exif.c when processing a crafted file.

CVE-2021-3496 has been assigned by [patrick@puiterwijk.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
[Security] heap-buffer-overflow of exif.c in function Get16u · Issue #33 · Matthias-Wandel/jhead · GitHub	github.com text/html	MISC github.com/Matthias-Wandel/jhead/issues/33
JHead: Multiple Vulnerabilities (GLSA 202210-17) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202210-17

1949245 – (CVE-2021-3496) CVE-2021-3496 jhead: heap-based buffer overflow in Get16u() in exif.c

[bugzilla.redhat.com](https://bugzilla.redhat.com/text/html)
text/html

MISC
bugzilla.redhat.com/show_bug.cgi?id=1949245

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

[179551](#) Debian Security Update for jhead (CVE-2021-3496)

[199565](#) Ubuntu Security Notification for Jhead Vulnerabilities (USN-6110-1)

[710664](#) Gentoo Linux JHead Multiple Vulnerabilities (GLSA 202210-17)

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

[750255](#) OpenSUSE Security Update for jhead (openSUSE-SU-2021:0594-1)

Exploit/POC from Github

A heap-based buffer overflow was found in jhead in version 3.06 in Get16u() in exif.c when processing a crafted file....

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jhead Project	Jhead	3.06	All	All	All
cpe:2.3:a:jhead_project:jhead:3.06:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID Next ID →		

© CVE.report 2023   |

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](#).

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