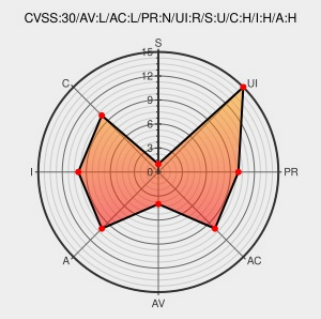
CVE-2018-17088

Published on: 09/16/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:19 PM UTC

CVE-2018-17088

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 there is an integer overflow during a check for whether a location exceeds the EXIF data length. This is analogous to the CVE-2016-3822 integer overflow in exif.c. This gpsinfo.c vulnerability is unrelated to the CVE-2018-16554 gpsinfo.c vulnerability.

CVE-2018-17088 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	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
#907925 - jhead: CVE-2018-17088: Integer overflow in gpsinfo.c	Exploit	MISC bugs.debian.org/cgi-bin/bugreport.cgi?

#907925 - jhead: CVE-2018-17088: Integer overflow in gpsinfo.c while running jhead - Debian Bug report logs	Exploit Mailing List Patch Third Party Advisory bugs.debian.org text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=907925
[SECURITY] [DLA 2054-1] jhead security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20191231 [SECURITY] [DLA 2054-1] jhead security update

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→