# chafa: NULL Pointer Dereference in function gif_internal_decode_frame at libnsgif.c:599 allows attackers to cause a denial of service (crash) via a crafted input file. in hpjansson/chafa

2

Valid Reported on Apr 20th 2022

## Steps to reproduce the issue

git clone https://github.com/hpjansson/chafa.git
cd chafa
export CFLAGS="-g -O0" export CXXFLAGS="-g -O0" ./autogen.sh ./configure --disable-shared
make
./tools/chafa/chafa ./poc.gif
gdb --args ./tools/chafa/chafa ./poc.gif
https://github.com/JieyongMa/poc/raw/main/gdb.jpg

## Proof of Concept

https://github.com/JieyongMa/poc/raw/main/poc.gif

## Impact

chafa: NULL Pointer Dereference in function gif_internal_decode_frame at libnsgif.c:599 allows attackers to cause a denial of service (crash) via a crafted input file.

CVE
CVE-2022-1507
(Published)

Vulnerability Type
CWE-476: NULL Pointer Dereference

Severity
Medium (5.5)

Registry

Registry
Other

Affected Version

<=1.10.1

Visibility
Public

Status
Fixed

Found by

TDHX ICS Security

@jieyongma

pro

This report was seen 674 times.

We are processing your report and will contact the **hpjansson/chafa** team within 24 hours. 7 months ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 7 months ago

We have contacted a member of the **hpjansson/chafa** team and are waiting to hear back 7 months ago

Hans 7 months ago Maintainer

Hi, thanks for reporting this. I've verified the issue and am working on a fix.

**Hans Petter Jansson** validated this vulnerability 7 months ago

**TDHX ICS Security** has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

**Hans Petter Jansson** marked this as fixed in **1.10.2** with commit **e4b777** 7 m

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Jamie Slome 7 months ago Admin

@maintainer - are you happy for us to assign and publish a CVE for this?

Hans 7 months ago Maintainer

Feel free :-) I'm happy to have the support in securing Chafa and the platform more generally, with all it entails.

Jamie Slome 7 months ago Admin

@Hans - amazing!

Feel free to drop our badge on your repository to let your community know they can win bounties for finding and fixing vulnerabilities in your repository!

```
[![huntr](https://cdn.huntr.dev/huntr_security_badge_mono.svg)](https://huntr.dev)
```


Jamie Slome 7 months ago Admin

CVE assigned and published! 🎉

Sign in to join this conversation