huntr

Heap-based Buffer Overflow in strukturag/libde265

1

✓ Valid Reported on May 12th 2021

✍️ Description

heap-buffer-overflow of decctx.cc in function read_sps_NAL

🕵️ Proof of Concept

Verification steps： 1.Get the source code of Bento4 2.Compile the Bento4

```
$ ./autogen.sh
$ export CFLAGS="-g -lpthread -fsanitize=address"
$ export CXXFLAGS="-g -lpthread -fsanitize=address"
$ CC=clang CXX=clang++ ./configure --disable-shared
$ make -j 32
```

3.run

```
$./dec265 poc
```

💥 Impact

This vulnerability is capable of DDOS or code execution

References

- https://github.com/strukturag/libde265/issues/293

CVE
CVE-2022-1253
(Published)

Vulnerability Type

CWE-122: Heap-based Buffer Overflow

Severity

High (7.4)

Affected Version

*

Visibility

Public

Status

Fixed

Found by

RouX

@nigelx

unranked

Fixed by

Dirk Farin

@farindk

maintainer

This report was seen 999 times.

Dirk Farin 8 months ago Maintainer

Fixed in 8e89fe0e175d2870c39486fdd09250b230ec10b8

Jamie Slome 8 months ago Admin

@farindk - thanks for the information. Would you be able to approve and confirm the fix using the action buttons in the drop-down section above?

Dirk Farin validated this vulnerability 8 months ago

RouX has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

Dirk Farin marked this as fixed in 1.0.8 with commit 8e89fe 8 months ago

Dirk Farin has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation