# Problem 2

## 1. Project Name

ImageMagick

## 2. Source Code Version

Version 7.0.6.0
https://github.com/ImageMagick/ImageMagick/releases/tag/7.0.6-0

## 3. PoC Downloadable from Internet?

Yes

## 4. CVE ID

CVE-2017-16546

## 5. Details Procedures that trigger the crash

### a. How the project program is compiled.

The program is compiled using the installation method described by the GitHub source:

1. Go to the directory of the project program and type:
2. make
3. sudo make install
4. magick --version

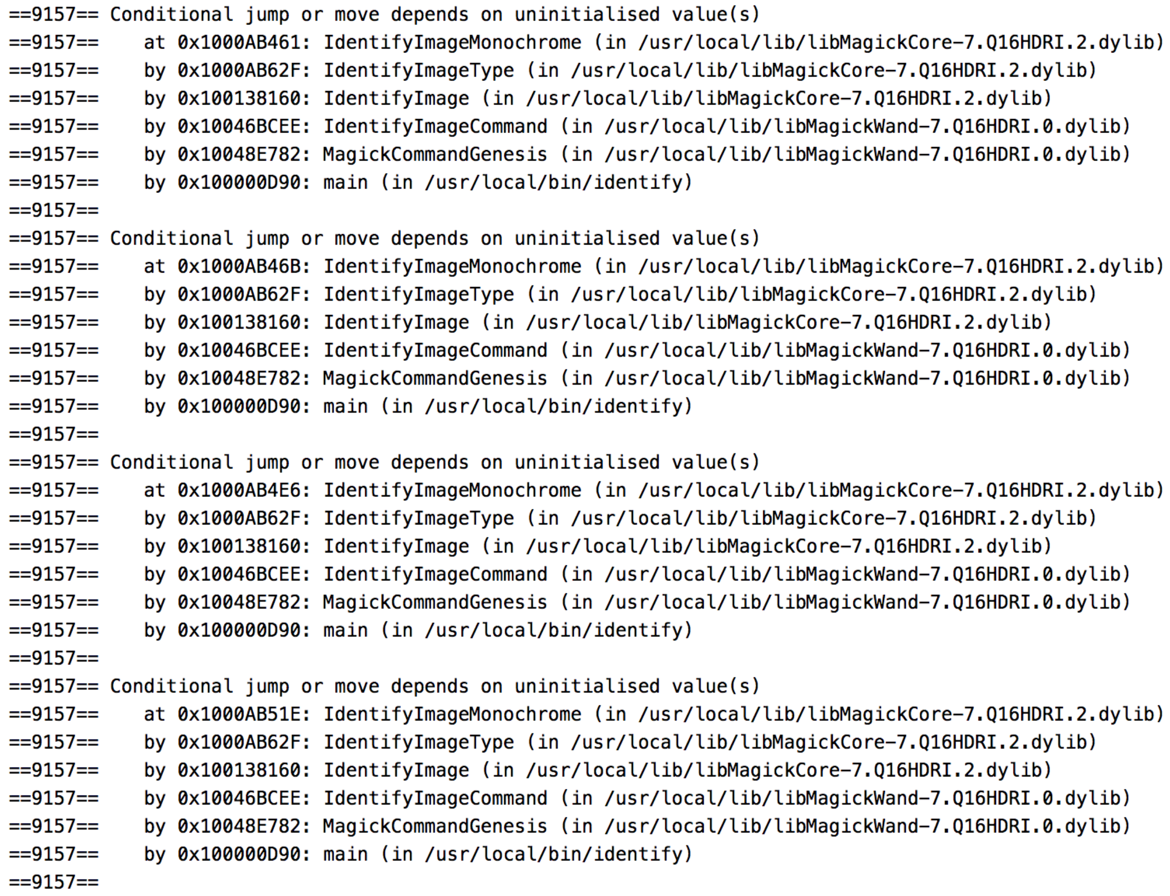
### b. The exact running arguments

1. Add in the input file “poc1.wpg”
2. Type: “valgrind identify -verbose in/poc1.wpg” on a malformed WPG file.

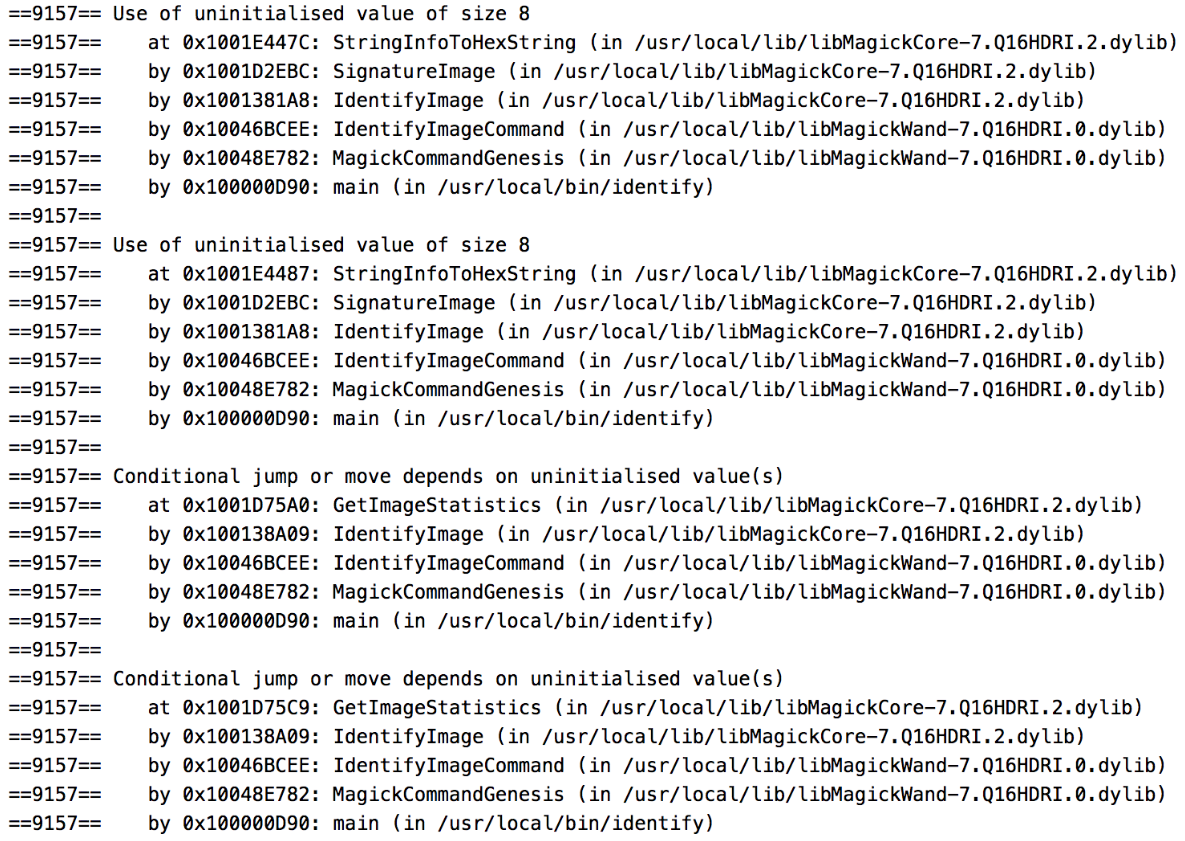
## Crash Description

The crash occurs due to multiple Heap Allocation errors. This is caused by uninitialized integers being allocated memory and the conditional jumps that depend on the uninitialized values, triggered by the verbose identify function being run on a malformed input image file.

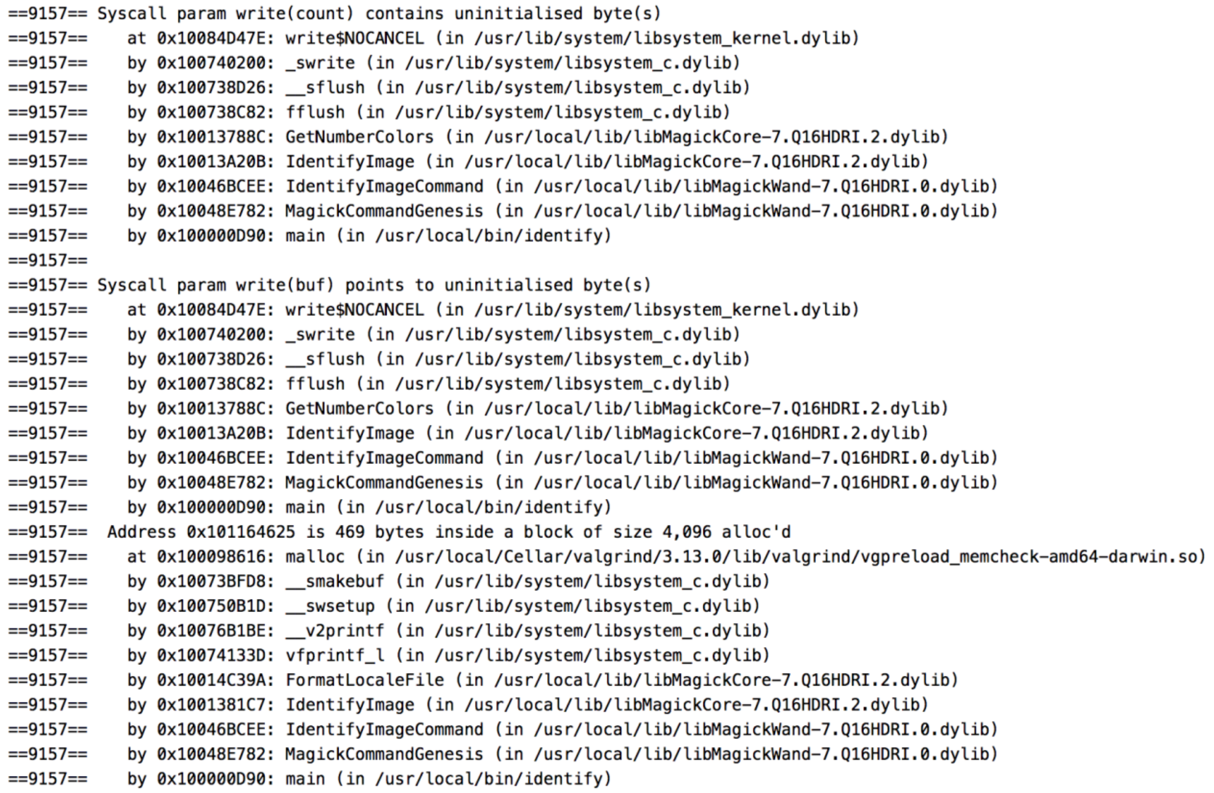
Some examples of conditional jumps and integers are shown below (refer to output file for full report):



```
==9157== Conditional jump or move depends on uninitialised value(s)
==9157==    at 0x1000AB461: IdentifyImageMonochrome (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x1000AB62F: IdentifyImageType (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x100138160: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
==9157==
==9157== Conditional jump or move depends on uninitialised value(s)
==9157==    at 0x1000AB46B: IdentifyImageMonochrome (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x1000AB62F: IdentifyImageType (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x100138160: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
==9157==
==9157== Conditional jump or move depends on uninitialised value(s)
==9157==    at 0x1000AB4E6: IdentifyImageMonochrome (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x1000AB62F: IdentifyImageType (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x100138160: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
==9157==
==9157== Conditional jump or move depends on uninitialised value(s)
==9157==    at 0x1000AB51E: IdentifyImageMonochrome (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x1000AB62F: IdentifyImageType (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x100138160: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
==9157==
```



```
==9157== Use of uninitialised value of size 8
==9157==    at 0x1001E447C: StringInfoToHexString (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x1001D2EBC: SignatureImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x1001381A8: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
==9157==
==9157== Use of uninitialised value of size 8
==9157==    at 0x1001E4487: StringInfoToHexString (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x1001D2EBC: SignatureImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x1001381A8: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
==9157==
==9157== Conditional jump or move depends on uninitialised value(s)
==9157==    at 0x1001D75A0: GetImageStatistics (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x100138A09: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
==9157==
==9157== Conditional jump or move depends on uninitialised value(s)
==9157==    at 0x1001D75C9: GetImageStatistics (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x100138A09: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
```



```
==9157== Syscall param write(count) contains uninitialised byte(s)
==9157==    at 0x10084D47E: write$NOCANCEL (in /usr/lib/system/libsystem_kernel.dylib)
==9157==    by 0x100740200: _swrite (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x100738D26: __sflush (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x100738C82: fflush (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x10013788C: GetNumberColors (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10013A20B: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
==9157==
==9157== Syscall param write(buf) points to uninitialised byte(s)
==9157==    at 0x10084D47E: write$NOCANCEL (in /usr/lib/system/libsystem_kernel.dylib)
==9157==    by 0x100740200: _swrite (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x100738D26: __sflush (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x100738C82: fflush (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x10013788C: GetNumberColors (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10013A20B: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
==9157==  Address 0x101164625 is 469 bytes inside a block of size 4,096 alloc'd
==9157==    at 0x100098616: malloc (in /usr/local/Cellar/valgrind/3.13.0/lib/valgrind/vgpreload_memcheck-amd64-darwin.so)
==9157==    by 0x10073BFD8: __smakebuf (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x100750B1D: __swsetup (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x10076B1BE: __v2printf (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x10074133D: vfprintf_l (in /usr/lib/system/libsystem_c.dylib)
==9157==    by 0x10014C39A: FormatLocaleFile (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x1001381C7: IdentifyImage (in /usr/local/lib/libMagickCore-7.Q16HDRI.2.dylib)
==9157==    by 0x10046BCEE: IdentifyImageCommand (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x10048E782: MagickCommandGenesis (in /usr/local/lib/libMagickWand-7.Q16HDRI.0.dylib)
==9157==    by 0x100000D90: main (in /usr/local/bin/identify)
```

# Brief explanation about bug fixed.

The bug is fixed by having an exception to check for corrupted or malformed image files as well as checking if the starting index is greater than the number of entries.