

DCMTK - Bug #942

Malformed data may cause out-of-bound read in dulparse.cc

2020-08-21 11:16 - Marco Eichelberg

Status:	Closed	Start date:	2020-08-21
Priority:	High	Due date:	
Assignee:		% Done:	100%
Category:	Library and Apps	Estimated time:	2:00 hours
Target version:		Compiler:	
Module:	dcmnet		
Operating System:			

Description

Short description of the bug

Certain network messages cause the vulnerable binary to perform out-of-bounds read access. The while statement in ofstd.cc:223 traverses the source buffer until it hits a null-byte string to calculate the length of the source buffer string. When copying plain not null-terminated data with the my_strncpy function in question, the source buffer is read past its bounds. The use of my_strncpy in the following bug prone call is copying data with a previously read length at dulparse.cc:739

```
OFStandard::strncpy(role->SOPClassUID, (char*)buf, UIDLength+1 /* +1 for 0-byte */);
```

Steps to reproduce

Download and extract DCMTK 3.6.5

```
wget ftp://dicom.offis.de/pub/dicom/offis/software/dcmtk/dcmtk365/dcmtk-3.6.5.tar.gz
tar -xvzf dcmtk-3.6.5.tar.gz
cd dcmtk-3.6.5
```

Apply patch to avoid undefined behavior in test suite
Copy the file `arith.patch` into the `dcmtk-3.6.5` folder.

```
patch config/tests/arith.cc arith.patch
```

Build DCMTK

```
CFLAGS="-funroll-loops -fno-omit-frame-pointer -O0 -g -fsanitize=address,undefined -fsanitize-recover=address,undefined" CXXFLAGS="-funroll-loops -fno-omit-frame-pointer -O0 -g -fsanitize=address,undefined -fsanitize-recover=address,undefined" cmake -DCMAKE_BUILD_TYPE=DEBUG -DCMAKE_C_COMPILER=gcc -DCMAKE_CXX_COMPILER=g++
CC=gcc CXX=g++ CFLAGS="-funroll-loops -fno-omit-frame-pointer -O0 -g -fsanitize=address,undefined -fsanitize-recover=address,undefined" CXXFLAGS="-funroll-loops -fno-omit-frame-pointer -O0 -g -fsanitize=address,undefined -fsanitize-recover=address,undefined" LDFLAGS="-funroll-loops -fno-omit-frame-pointer -O0 -g -fsanitize=address,undefined -fsanitize-recover=address,undefined" nice -n 19 make -j$ (nproc)
```

Serve network input via `netcat-openbsd`

```
nc -Nl 12345 < input_vector
```

Create an empty input query

```
touch empty
```

Execute findscu with empty input

```
ASAN_OPTIONS=detect_leaks=0 bin/findscu --cancel 1 -to 1 -td 1 -ta 1 -ll trace 1 ocalhost 12345 empty
```

Reported 2020-08-20 by Matthias Gierlings <matthias.gierlings@ruhr-uni-bochum.de>.

History

#1 - 2020-09-13 15:17 - Marco Eichelberg

- Status changed from New to Closed
- % Done changed from 0 to 100
- Estimated time set to 2:00 h

Closed by commit #10428a74e.

Files

arith.patch	556 Bytes	2020-08-21	Marco Eichelberg
input_vector	188 Bytes	2020-08-21	Marco Eichelberg
trace.txt	10.1 KB	2020-08-21	Marco Eichelberg