New issue

Jump to bottom

# UPF crashes after UDP port scan #1767

Closed **Popvlvs** opened this issue on Sep 19 · 6 comments

Labels Security

**Popvlvs** commented on Sep 19

Hi all,

First of all, I'd like to analyze this issue deeply, because I got this in the very first test. However, it seems really easy to achieve a DoS attack by executing a simple port scan.

Following image shows the UPF log after the scan:

```
09/19 08:04:02.066: [upf] INFO: [Removed] Number of UPF-sessions is now 1 (../src/upf/context.c:212)
09/19 08:04:04.627: [upf] INFO: [Added] Number of UPF-Sessions is now 2 (../src/upf/context.c:178)
09/19 08:04:04.676: [upf] INFO: UE F-SEID[CP:0x4 UP:0xa] APN[internet] PDN-Type[1] IPv4[10.45.0.11] IPv6[] (../src/upf/context.c:397)
09/19 08:24:07.038: [upf] ERROR: ogs_recvfrom() failed (../src/upf/pfcp-path.c:79)
09/19 08:24:08.343: [upf] ERROR: ogs_recvfrom() failed (../src/upf/pfcp-path.c:79)
09/19 08:24:08.771: [upf] ERROR: [DROP] Invalid GTPU version [3] (../src/upf/gtp-path.c:250)
0000: 72fe1d13 00000000 00000002 000186a0   r...............
0010: 0001977c 00000000 00000000 00000000   ...|............
0020: 00000000 00000000                     ........
09/19 08:24:08.772: [upf] ERROR: Not supported version[3] (../src/upf/pfcp-path.c:91)
09/19 08:24:13.784: [pfcp] INFO: ogs_pfcp_connect() [10.250.250.1]:54855 (../lib/pfcp/path.c:61)
09/19 08:24:13.784: [upf] ERROR: [DROP] Invalid GTPU version [0] (../src/upf/gtp-path.c:250)
0000: 00060100 00010000 00000000 07766572   .............ver
0010: 73696f6e 0462696e 64000010 0003       sion.bind.....
09/19 08:24:13.784: [tlv] FATAL: ogs_tlv_parse_block: Assertion `length == (pos - blk)' failed. (../lib/core/ogs-tlv.c:464)
09/19 08:24:13.843: [core] FATAL: backtrace() returned 10 addresses (../lib/core/ogs-abort.c:37)
/home/core5g/open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(ogs_tlv_parse_block+0x2c6) [0x7fbe7832f494]
/home/core5g/open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(ogs_tlv_parse_msg+0x224) [0x7fbe783321ba]
/home/core5g/open5gs/install/lib/x86_64-linux-gnu/libogspfcp.so.2(ogs_pfcp_parse_msg+0x41a) [0x7fbe781ff7e0]
/home/core5g/open5gs/install/bin/open5gs-upfd(+0xb814) [0x558bddef4814]
/home/core5g/open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(ogs_fsm_dispatch+0xab) [0x7fbe78332c5a]
/home/core5g/open5gs/install/bin/open5gs-upfd(+0x7423) [0x558bddef0423]
/home/core5g/open5gs/install/lib/x86_64-linux-gnu/libogscore.so.2(+0x12639) [0x7fbe78324639]
/lib/x86_64-linux-gnu/libpthread.so.0(+0x8609) [0x7fbe77eee609]
/lib/x86_64-linux-gnu/libc.so.6(clone+0x43) [0x7fbe77e13133]
```

I'll update this thread with further discoveries.

Regards.

**Popvlvs** changed the title ~~**UDM crahses after UDP port scan**~~ **UPFcrahses after UDP port scan** on Sep 19

**Popvlvs** changed the title ~~**UPFcrahses after UDP port scan**~~ **UPF crashes after UDP port scan** on Sep 19

**acetcom** added the Bug label on Sep 24

**acetcom** added a commit that referenced this issue on Sep 24

`[TLV] Added more debug information (#1767)` ✓ `c2f6a02`

**acetcom** added the **Not Enough** label on Sep 24

**acetcom** commented on Sep 24 — Member

**@Popvlvs**

I've added more debug information to fix this issue in the main branch. If you can reproduce this problem, please share the print log message.

Thanks a lot!
Sukchan

**acetcom** added Security and removed **Not Enough** Bug labels on Sep 27

**acetcom** commented on Sep 28 — Member

**@Popvlvs**

I've improved the security protection in the branch issues1767.

Please let me know if the issue has been resolved.

Thanks a lot!
Sukchan

**Popvlvs** commented on Sep 28 — Author

**@acetcom**

It fails when compiling. See the following picture:

```
ninja: Entering directory `build'
[3090/3241] Linking target src/amf/open5gs-amfd.
FAILED: src/amf/open5gs-amfd
cc  -o src/amf/open5gs-amfd 'src/amf/b58c9c5@@open5gs-amfd@exe/app.c.o' 'src/amf/b58c9c5@@open5gs-amfd@exe/._main.c.o' -Wl,--as-needed -Wl,--no
-undefined -Wl,--start-group src/amf/libamf.a lib/metrics/libogsmetrics.so.2.4.10 lib/app/libogsapp.so.2.4.10 lib/core/libogscore.so.2.4.10 lib/
sctp/libogssctp.so.2.4.10 lib/ngap/libogsngap.so.2.4.10 lib/asn1c/ngap/libogsasn1c-ngap.so.2.4.10 lib/asn1c/common/libogsasn1c-common.so.2.4.10
lib/asn1c/util/libogsasn1c-util.so.2.4.10 lib/nas/5gs/libogsnas-5gs.so.2.4.10 lib/nas/common/libogsnas-common.so.2.4.10 lib/crypt/libogscrypt.so
.2.4.10 lib/proto/libogsproto.so.2.4.10 lib/sbi/libogssbi.so.2.4.10 lib/sbi/openapi/libogssbi-openapi.so.2.4.10 -pthread /usr/lib/x86_64-linux-g
nu/libtalloc.so /usr/lib/x86_64-linux-gnu/libyaml.so -lsctp -lgnutls /usr/lib/x86_64-linux-gnu/libnghttp2.so /usr/lib/x86_64-linux-gnu/libmicroh
ttpd.so /usr/lib/x86_64-linux-gnu/libcurl.so -lsctp -lgnutls -Wl,--end-group '-Wl,-rpath,$ORIGIN/:$ORIGIN/../../lib/metrics:$ORIGIN/../../lib/ap
p:$ORIGIN/../../lib/core:$ORIGIN/../../lib/sctp:$ORIGIN/../../lib/ngap:$ORIGIN/../../lib/asn1c/ngap:$ORIGIN/../../lib/asn1c/common:$ORIGIN/../..
/lib/asn1c/util:$ORIGIN/../../lib/nas/5gs:$ORIGIN/../../lib/nas/common:$ORIGIN/../../lib/crypt:$ORIGIN/../../lib/proto:$ORIGIN/../../lib/sbi:$OR
IGIN/../../lib/sbi/openapi' -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/src/amf -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/
lib/metrics -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/lib/app -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/lib/core -Wl,-rp
ath-link,/home/core5g/open5gs_issues1767/build/lib/sctp -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/lib/ngap -Wl,-rpath-link,/home/cor
e5g/open5gs_issues1767/build/lib/asn1c/ngap -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/lib/asn1c/common -Wl,-rpath-link,/home/core5g/
open5gs_issues1767/build/lib/asn1c/util -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/lib/nas/5gs -Wl,-rpath-link,/home/core5g/open5gs_i
ssues1767/build/lib/nas/common -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/lib/crypt -Wl,-rpath-link,/home/core5g/open5gs_issues1767/b
uild/lib/proto -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/lib/sbi -Wl,-rpath-link,/home/core5g/open5gs_issues1767/build/lib/sbi/opena
pi
collect2: error: ld returned 1 exit status
[3091/3241] Compiling C object 'tests/core/80aa9e8@@core@exe/log-test.c.o'.
ninja: build stopped: subcommand failed.
```

Regards.

**acetcom** commented on Sep 28 — Member

**@Popvlvs**

Here are my results.

```
$ rm -Rf open5gs
$ git clone https://github.com/open5gs/open5gs
$ cd open5gs
$ git checkout issues1767
Branch 'issues1767' set up to track remote branch 'issues1767' from 'origin'.
Switched to a new branch 'issues1767'
$ meson build --prefix=`pwd`/install
$ cd build
$ ninja
[3241/3241] Linking target tests/non3gpp/non3gpp.
```

That works well.

Good luck with you!
Sukchan

**Popvlvs** commented on Sep 28 — Author

**@acetcom**

My fault :)

It seems it's fixed now. It logs errors because of the malformed UDP payload (as expected) but it doesn't crash. Besides, I tried to register a new UE during the port scan and it attaches to the network successfully (highlighted on the following picture).

```
09/28 08:38:30.037: [upf] ERROR: Not supported version[3] (../src/upf/pfcp-path.c:89)
09/28 08:38:34.996: [upf] ERROR: [DROP] Invalid GTPU version [0] (../src/upf/gtp-path.c:250)
0000: 1b00003d 00000000 12434f4e 4e454354   ...=.....CONNECT
0010: 494f4e4c 4553535f 54445300 00000100   IONLESS_TDS.....
0020: 00040005 00050000 01020000 03010104   ................
0030: 08000000 00000000 00070204 b1         .............
09/28 08:38:34.998: [upf] ERROR: Not supported version[0] (../src/upf/pfcp-path.c:89)
09/28 08:38:37.747: [upf] INFO: [Removed] Number of UPF-sessions is now 0 (../src/upf/context.c:212)
09/28 08:38:37.969: [upf] INFO: [Added] Number of UPF-Sessions is now 1 (../src/upf/context.c:178)
09/28 08:38:37.969: [upf] INFO: UE F-SEID[CP:0x3 UP:0x3] APN[internet] PDN-Type[1] IPv4[10.45.0.4] IPv6[] (../src/upf/context.c:397)
09/28 08:38:37.969: [upf] INFO: UE F-SEID[CP:0x3 UP:0x3] APN[internet] PDN-Type[1] IPv4[10.45.0.4] IPv6[] (../src/upf/context.c:397)
09/28 08:38:40.000: [upf] ERROR: [DROP] Invalid GTPU version [0] (../src/upf/gtp-path.c:250)
0000: 00405000 00000085 5db49128 00000000   .@P.....]..(....
0010: 00017c91 40000000 aa39da42 3765cf01   ..|.@....9.B7e..
0020: 00000000 00000000 00000000 00000000   ................
0030: 00000000 00000000 00000000 00000000   ................
09/28 08:38:40.000: [upf] ERROR: Not supported version[0] (../src/upf/pfcp-path.c:89)
09/28 08:38:45.003: [upf] ERROR: [DROP] Invalid GTPU version [0] (../src/upf/gtp-path.c:250)
0000: 16feff00 00000000 00000000 36010000   ............6...
0010: 2a000000 00000000 2afefd00 0000007c   *.......*......|
0020: 77401e8a c822a0a0 18ff9308 caac0a64   w@...".........d
0030: 2fc92264 bc08a816 89193000 00000200   /."d......0.....
0040: 2f0100                                /..
09/28 08:38:45.004: [upf] ERROR: Not supported version[0] (../src/upf/pfcp-path.c:89)
09/28 08:38:50.005: [upf] ERROR: [DROP] Invalid GTPU version [0] (../src/upf/gtp-path.c:250)
0000: 0d89c19c 1c2afffc f1513939 3900       .....*...Q999.
09/28 08:38:50.007: [upf] ERROR: Not supported version[0] (../src/upf/pfcp-path.c:89)
09/28 08:38:55.016: [upf] ERROR: [DROP] Invalid GTPU Type [40] (../src/upf/gtp-path.c:580)
0000: 000186a0 00000002 00000000 00000000   ................
0010: 00000000 00000000 00000000            ............
09/28 08:38:55.020: [pfcp] INFO: ogs_pfcp_connect() [192.168.0.204]:62707 (../lib/pfcp/path.c:61)
09/28 08:38:55.020: [pfcp] WARNING: Not implemented(type:225) (../lib/pfcp/message.c:4107)
09/28 08:38:55.020: [upf] ERROR: ogs_pfcp_parse_msg() failed (../src/upf/upf-sm.c:70)
```

Thanks again!

Regards.

👍 1

**acetcom** added a commit that referenced this issue on Oct 1

[Security] Fixed a crash for port scanning (#1767) ✓ 71a1516

**acetcom** commented on Oct 1 — Member

**@Popvlvs**

I've merge it to the main branch.

Thank you so much!
Sukchan

**Popvlvs** closed this as completed on Oct 4

**NLag** added a commit to securitylab-repository/open5gs_ciot that referenced this issue on Oct 19

Update repo to open5gs/open5gs main (#1) ... fdfe2c9

**Assignees**

No one assigned

**Labels**

Security

**Projects**

None yet

**Milestone**

No milestone

**Development**

No branches or pull requests

**2 participants**