OsmoSGSN - Bug #2960

OsmoSGSN confirms PDP CTX ACT to MS/Gb despite missing conditional IEs on GTP

02/17/2018 09:23 PM - laforge

Status:	New	**Start date:**	02/17/2018
Priority:	Normal	**Due date:**	
Assignee:	lynxis	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

When the GTP Create PDP Context Response is positive but missing some conditional IE (e.g. GTPIE_CHARGING_ID), we end up in a weird state where we

- Confirm PDP CTX activation to the MS, i.e. Gb/Um side thinks the PDP context is active
- Continue to re-transmit CreatePDP Context Requests to the GGSN
  - Eventually those attempts time out
  - we then send a PDP CTX Activate Reject **after** we already confirmed it before

```
Sat Feb 17 22:15:20 2018 DLGLOBAL <001d> telnet_interface.c:104 telnet at 127.0.0.1 4245
Sat Feb 17 22:15:20 2018 DLCTRL <0024> control_if.c:854 CTRL at 127.0.0.1 4251
Sat Feb 17 22:15:20 2018 DLGTP <0025> gtp.c:757 GTP: gtp_newgsn() started at 127.0.0.1
Sat Feb 17 22:15:20 2018 DGPRS <000f> sgsn_libgtp.c:839 Created GTP on 127.0.0.1
Sat Feb 17 22:15:20 2018 DGPRS <000f> sgsn_main.c:478 libGTP v1.1.0 initialized
Sat Feb 17 22:15:20 2018 DLGSUP <0027> gsup_client.c:76 GSUP connecting to 127.0.0.1:4222
Sat Feb 17 22:15:20 2018 DNS <0010> gprs_ns.c:1628 Listening for nsip packets on 127.0.0.1:23000
Sat Feb 17 22:15:20 2018 DNS <0010> gprs_ns.c:1641 NS UDP socket at 127.0.0.1:23000
Sat Feb 17 22:15:30 2018 DLGSUP <0027> gsup_client.c:76 GSUP connecting to 127.0.0.1:4222
Sat Feb 17 22:15:34 2018 DBSSGP <0011> gprs_bssgp.c:289 Cell 262-42-13135-0 CI 20960 on BVCI 196
Sat Feb 17 22:15:40 2018 DLGSUP <0027> gsup_client.c:76 GSUP connecting to 127.0.0.1:4222
Sat Feb 17 22:15:40 2018 DLINP <001f> input/ipa.c:129 connection done.
Sat Feb 17 22:15:40 2018 DLINP <001f> input/ipaccess.c:707 received ID get
Sat Feb 17 22:15:40 2018 DLLC <0012> gprs_llc.c:526 LLC RX: unknown TLLI 0xd8c18acb, creating LLME
 on the fly
Sat Feb 17 22:15:40 2018 DLLC <0012> gprs_llc_parse.c:81 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS
=0x24bf94 CMD=UI DATA
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:1271 MM(---/ffffffff) -> GMM ATTACH REQUEST MI(2624
20000000017) type="GPRS attach"
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_sgsn.c:237 MM(/00000000) Allocated with GEA0 cipher.
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:556 MM(262420000000017/fd9e8165) <- GPRS IDENTITY R
EQUEST: mi_type=IMEI
Sat Feb 17 22:15:40 2018 DLLC <0012> gprs_llc_parse.c:81 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS
=0x612fca CMD=UI DATA
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:1194 MM(262420000000017/fd9e8165) -> GMM IDENTITY R
ESPONSE: MI(IMEI)=499990000000017
Sat Feb 17 22:15:40 2018 DMM <0002> sgsn_auth.c:160 MM(262420000000017/fd9e8165) Requesting author
ization
Sat Feb 17 22:15:40 2018 DMM <0002> sgsn_auth.c:185 MM(262420000000017/fd9e8165) Requesting authen
tication tuples
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_subscriber.c:894 MM(262420000000017/fd9e8165) Requesting
 subscriber authentication info
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_sgsn.c:726 MM(262420000000017/fd9e8165) Subscriber data u
pdate
Sat Feb 17 22:15:40 2018 DMM <0002> sgsn_auth.c:219 MM(262420000000017/fd9e8165) Updating authoriz
ation (unknown -> authenticate)
Sat Feb 17 22:15:40 2018 DMM <0002> sgsn_auth.c:248 MM(262420000000017/fd9e8165) Got authorization
 update: state unknown -> authenticate
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:591 MM(262420000000017/fd9e8165) <- GPRS AUTH AND C
IPHERING REQ (rand = 2c 6b 09 d8 c4 fd f6 42 b0 82 a8 99 dc 4b cc e5 )
Sat Feb 17 22:15:40 2018 DLLC <0012> gprs_llc_parse.c:81 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS
=0xe62da8 CMD=UI DATA
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:731 MM(262420000000017/fd9e8165) -> GPRS AUTH AND C
```

```
IPH RESPONSE
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:778 MM(262420000000017/fd9e8165) checking auth: rec
eived GSM SRES = c2 82 3f 50
Sat Feb 17 22:15:40 2018 DMM <0002> sgsn_auth.c:160 MM(262420000000017/fd9e8165) Requesting author
ization
Sat Feb 17 22:15:40 2018 DMM <0002> sgsn_auth.c:196 MM(262420000000017/fd9e8165) Missing informati
on, requesting subscriber data
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_subscriber.c:869 MM(262420000000017/fd9e8165) Requesting
subscriber data update
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_sgsn.c:726 MM(262420000000017/fd9e8165) Subscriber data u
pdate
Sat Feb 17 22:15:40 2018 DMM <0002> sgsn_auth.c:219 MM(262420000000017/fd9e8165) Updating authoriz
ation (authenticate -> accepted)
Sat Feb 17 22:15:40 2018 DMM <0002> sgsn_auth.c:248 MM(262420000000017/fd9e8165) Got authorization
 update: state authenticate -> accepted
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:1118 MM(262420000000017/fd9e8165) Authorized, conti
nuing procedure, IMSI=262420000000017
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:437 MM(262420000000017/fd9e8165) <- GPRS ATTACH ACC
EPT (new P-TMSI=0xfd9e8165)
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_sgsn.c:726 MM(262420000000017/fd9e8165) Subscriber data u
pdate
Sat Feb 17 22:15:40 2018 DMM <0002> sgsn_auth.c:219 MM(262420000000017/fd9e8165) Updating authoriz
ation (accepted -> accepted)
Sat Feb 17 22:15:40 2018 DLLC <0012> gprs_llc_parse.c:81 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS
=0xffae8e CMD=UI DATA
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:1997 MM(262420000000017/fd9e8165) -> ATTACH COMPLET
E
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:165 MM(262420000000017/fd9e8165) Changing MM state
from MM IDLE to MM READY
Sat Feb 17 22:15:40 2018 DLLC <0012> gprs_llc_parse.c:81 LLC SAPI=1 C   U GEA0 IOV-UI=0x000000 FCS
=0x540e4a CMD=UI DATA
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:2445 MM(262420000000017/fd9e8165) -> ACTIVATE PDP C
ONTEXT REQ: SAPI=3 NSAPI=5 IETF IPv4
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_sgsn.c:876 MM(262420000000017/fd9e8165) Found GGSN 0 for
APN '' (requested '')
Sat Feb 17 22:15:40 2018 DMM <0002> gprs_gmm.c:2332 MM(262420000000017/fd9e8165) Using GGSN 0
Sat Feb 17 22:15:40 2018 DGPRS <000f> sgsn_libgtp.c:176 PDP(262420000000017/0) Create PDP Context
Sat Feb 17 22:15:40 2018 DLGTP <0025> gtp.c:1795 Packet from 127.0.0.2:2123, length: 49 content: 3
2 11 00 29 00 00 00 01 b0 00 00 00 01 80 08 00 10 00 02 00 00 11 00 01 00 00 14 05 85 00 04 7f 00
00 01 85 00 04 7f 00 00 01 87 00 04 00 0b 92 1f : Missing conditional information field
Sat Feb 17 22:15:40 2018 DGPRS <000f> sgsn_libgtp.c:619 libgtp EOF (type=16, pdp=0x7ff712ffc2e0, c
bp=0x55df997cee50)
Sat Feb 17 22:15:40 2018 DGPRS <000f> sgsn_libgtp.c:400 Create PDP ctx req timed out
Sat Feb 17 22:15:40 2018 DLLC <0012> gprs_llc.c:342 Sending XID type NULL (8 bytes) request to MS.
..
Sat Feb 17 22:15:40 2018 DLINP <001f> input/ipa.c:67 connection closed with server
Sat Feb 17 22:15:50 2018 DLGSUP <0027> gsup_client.c:76 GSUP connecting to 127.0.0.1:4222
Sat Feb 17 22:16:00 2018 DLGSUP <0027> gsup_client.c:76 GSUP connecting to 127.0.0.1:4222
Sat Feb 17 22:16:08 2018 DGPRS <000f> sgsn_libgtp.c:619 libgtp EOF (type=16, pdp=(nil), cbp=0x55df
997cee50)
Sat Feb 17 22:16:08 2018 DGPRS <000f> sgsn_libgtp.c:400 Create PDP ctx req timed out
Sat Feb 17 22:16:08 2018 DMM <0002> gprs_gmm.c:2258 MM(262420000000017/fd9e8165) <- ACTIVATE PDP C
ONTEXT REJ(cause=38)
```

History

#1 - 02/17/2018 09:28 PM - laforge

Upon second sight, this is the GTPv1 -> GTPv0 fallback mechanism.

So if the activation fails on GTPv1, we try it on GTPv1.

Of course we shouldn't report the failed v1 activation as success to the MS, though.

#2 - 02/17/2018 09:29 PM - laforge

- Subject changed from OsmoSGSN PDP context mismatch Gb vs. GTP on missing conditional IEs to OsmoSGSN confirms PDP CTX ACT to MS/Gb

despite missing conditional IEs on GTP

#3 - 05/17/2018 01:57 PM - laforge

- Assignee changed from sysmocom to lynxis

#4 - 04/15/2019 07:37 AM - laforge

Files

20180216-sgsn-pdp_ctx_act-missing_cond_ie.pcap	4.81 KB	02/17/2018	laforge