strongSwan - Bug #501

charon segfaults when switching configs due to failed authentication during IKEv1 Agressive Mode

26.01.2014 04:27 - ballack W

Status:	Closed	**Start date:**	26.01.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.1.2		
Affected version:	5.1.0	**Resolution:**	Fixed

Description

Strongswan-5.1.0
CentOS 6.3
gcc-4.4.6
glibc-2.12

I use eap-radius plugin to auth user's connection for IPSec, But the connection between ikev1 and client often failed, the log showed:

```
Jan 25 22:48:25 08[NET] received packet: from 223.240.212.251[4500] to 110.45.173.141[4500] (92 by
tes)
Jan 25 22:48:25 08[ENC] parsed INFORMATIONAL_V1 request 2487758038 [ HASH N(INITIAL_CONTACT) ]
Jan 25 22:48:25 08[IKE] calculated HASH does not match HASH payload
Jan 25 22:48:25 08[CFG] switching to peer config 'IKEv1-0'
Jan 25 22:48:25 08[IKE] calculated HASH does not match HASH payload
Jan 25 22:48:25 08[CFG] switching to peer config 'PureIPSec-IKEv1'
Jan 25 22:48:25 08[IKE] calculated HASH does not match HASH payload
Jan 25 22:48:25 08[CFG] no alternative config found
Jan 25 22:48:25 08[DMN] thread 8 received 11
Jan 25 22:48:25 08[LIB]  dumping 10 stack frame addresses:
Jan 25 22:48:25 08[LIB]    @ 0x658000 (__kernel_sigreturn+0x0) [0x658400]
Jan 25 22:48:25 08[LIB]   /lib/libc.so.6 @ 0x197000 [0x20a50f]
```

there is no output any more, ikev1,ikev2 and l2tp over ipsec cant work. I checked Bug #346, which is totally different from mine.

ipsec.conf

```
config setup
        uniqueids=never

conn %default
        ikelifetime=60m
        keylife=20m
        keyingtries=3
        rekeymargin=3m

conn IKEv1
        keyexchange=ikev1
        aggressive=yes
        modeconfig=push
        rekey=no
        auto=add
        dpdaction=clear
        dpddelay=300s
        dpdtimeout=1h
        type=tunnel
        leftid=ipsec
        leftauth=psk
        rightauth=psk
        rightauth2=xauth-eap
        compress=yes

conn IKEv2
```

```
        keyexchange=ikev2
        modeconfig=push
        auto=add
        rekey=no
        dpdaction=clear
        dpddelay=300s
        dpdtimeout=1h
        leftauth=pubkey
        leftcert=serverCert.pem
        rightauth=eap-radius
        rightsendcert=never
        eap_identity=%any
        compress=yes

conn L2TP-PSK-noNAT
        #leftfirewall=yes
        #rightfirewall=yes
    keyexchange=ikev1
    auto=add
        rekey=no
        dpdaction=clear
        dpddelay=300s
        dpdtimeout=1h
        type=transport
        right=%any
        authby=psk
        leftprotoport=17/1701
        rightprotoport=17/%any
        compress=yes
```

strongswan.conf

```
charon {
    i_dont_care_about_security_and_use_aggressive_mode_psk = yes
    install_virtual_ip = yes
    duplicheck.enable = no
     threads = 16

    dns1 = 8.8.8.8
    dns2 = 8.8.4.4

    filelog {
          /var/log/strongswan.log {
          time_format = %b %e %T
          flush_line = yes
              }
    }

    plugins {

        eap-radius {
            accounting = yes
            servers {
                radius {
                    address = my.radius.com
                    secret = mysecret
                    }
                }
            }

        xauth-eap {
            backend = radius
        }
    }
}
pluto {
}
```

```
libstrongswan {

}
```

Associated revisions

Revision 9e1ce639 - 12.02.2014 13:53 - Tobias Brunner

ikev1: Fix config switching due to failed authentication during Aggressive mode

The encoded ID payload gets destroyed by the authenticator, which caused
a segmentation fault after the switch.

Fixes #501.

History

#1 - 07.02.2014 10:12 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from charon suspended animation to charon segfaults when switching configs due to failed authentication during IKEv1 Agressive Mode

- Description updated

- Status changed from New to Feedback

- Assignee changed from Martin Willi to Tobias Brunner

- Priority changed from High to Normal

- Target version set to 5.1.2

What clients do you use? It's quite unusual that the PSK verification fails so late. Usually, the decryption of the message already fails.

Anyway, I was able to reproduce the crash. I pushed a fix (3dd310d87) to the *ikev1-switch-fix* branch of our repository. Let me know if this works for you.

#2 - 09.02.2014 06:19 - ballack W

Hi Tobias
xp system use shrew vpn client to connect ikev1, win7 system use the built-in dial-up connection components ikev2

#3 - 10.02.2014 02:20 - ballack W

Hi Tobias:
make error

```
./configure --prefix=/usr --sysconfdir=/etc --enable-eap-identity --enable-eap-md5 --enable-eap-mschapv2 --ena
ble-eap-tls --enab
le-eap-ttls --enable-eap-peap --enable-eap-tnc --enable-eap-dynamic --enable-eap-radius --enable-xauth-eap --e
nable-xauth-pa:q!
m --enable-dhcp --enable-openssl --enable-addrblock --enable-unity --enable-certexpire --enable-radattr --enab
le-tools --enable-
openssl --disable-gmp

make && make install

/bin/sh ../../libtool  --tag=CC   --mode=compile gcc -DHAVE_CONFIG_H -I. -I../..  -I../../src/include -I../../
src/libstrongswan -I../../src/libhydra -I../../src/libcharon -DIPSEC_DIR=\"/usr/libexec/ipsec\" -DIPSEC_PIDDIR
=\"/var/run\"   -g -O2 -Wall -Wno-format -Wno-pointer-sign -include /root/strongswan-5.1.0/config.h -MT aggres
sive_mode.lo -MD -MP -MF .deps/aggressive_mode.Tpo -c -o aggressive_mode.lo `test -f 'sa/ikev1/tasks/aggressiv
e_mode.c' || echo './'`sa/ikev1/tasks/aggressive_mode.c
libtool: compile:  gcc -DHAVE_CONFIG_H -I. -I../.. -I../../src/include -I../../src/libstrongswan -I../../src/l
ibhydra -I../../src/libcharon -DIPSEC_DIR=\"/usr/libexec/ipsec\" -DIPSEC_PIDDIR=\"/var/run\" -g -O2 -Wall -Wno
-format -Wno-pointer-sign -include /root/strongswan-5.1.0/config.h -MT aggressive_mode.lo -MD -MP -MF .deps/ag
gressive_mode.Tpo -c sa/ikev1/tasks/aggressive_mode.c  -fPIC -DPIC -o .libs/aggressive_mode.o
sa/ikev1/tasks/aggressive_mode.c: In function 'build_i':
sa/ikev1/tasks/aggressive_mode.c:340: error: 'peer_cfg_t' has no member named 'use_pull_mode'
sa/ikev1/tasks/aggressive_mode.c:343: error: too many arguments to function 'mode_config_create'
sa/ikev1/tasks/aggressive_mode.c:352: error: 'peer_cfg_t' has no member named 'use_pull_mode'
sa/ikev1/tasks/aggressive_mode.c:359: error: too many arguments to function 'mode_config_create'
sa/ikev1/tasks/aggressive_mode.c: In function 'process_r':
sa/ikev1/tasks/aggressive_mode.c:535: error: 'peer_cfg_t' has no member named 'use_pull_mode'
sa/ikev1/tasks/aggressive_mode.c:538: error: too many arguments to function 'mode_config_create'
sa/ikev1/tasks/aggressive_mode.c:543: error: 'peer_cfg_t' has no member named 'use_pull_mode'
```

```
sa/ikev1/tasks/aggressive_mode.c:546: error: too many arguments to function 'mode_config_create'
make[4]: *** [aggressive_mode.lo] Error 1
make[4]: Leaving directory `/root/strongswan-5.1.0/src/libcharon'
make[3]: *** [all-recursive] Error 1
make[3]: Leaving directory `/root/strongswan-5.1.0/src/libcharon'
make[2]: *** [all-recursive] Error 1
make[2]: Leaving directory `/root/strongswan-5.1.0/src'
make[1]: *** [all-recursive] Error 1
make[1]: Leaving directory `/root/strongswan-5.1.0'
make: *** [all] Error 2
```

#4 - 10.02.2014 13:00 - Tobias Brunner

```
sa/ikev1/tasks/aggressive_mode.c:543: error: 'peer_cfg_t' has no member named 'use_pull_mode'
sa/ikev1/tasks/aggressive_mode.c:546: error: too many arguments to function 'mode_config_create'
```

Support for push mode was added with 5.1.1. Did you just copy the updated aggressive_mode.c file from the new branch? This won't work, as you didn't get all the required changes in other files.

If you don't want to update, you should be able to apply the patch to 5.1.0. Go to 3dd310d87, click *View differences*, there click *Unified diff* at the bottom right. Then apply the patch with patch -p1 < /path/to/downloaded/patch.

#5 - 11.02.2014 08:32 - ballack W

Hi Tobias
Thanks so much, The compilation has been finished successfully, I will feedback the usage in time

#6 - 11.02.2014 08:33 - ballack W

I update 5.1.0 to 5.1.1

#7 - 12.02.2014 16:08 - Tobias Brunner

- Status changed from Feedback to Resolved

- Resolution set to Fixed

#8 - 28.02.2014 08:37 - ballack W

Hi Tobias:
I used the patch you updated, but I have got a problem, the server can be connected successfully while the connection will be dropped seconds later. my ipsec.conf,the client is shrew vpn client use push mode.

```
#ipsec.conf
config setup
        uniqueids=never

conn %default
        ikelifetime=60m
        keylife=20m
        keyingtries=3
        rekeymargin=3m

conn PureIPSec-IKEv2
        keyexchange=ikev2
        modeconfig=push
        dpdtimeout=1h
        dpddelay=300s
        dpdaction=clear
        auto=add
        rekey=no
        leftauth=pubkey
        leftcert=serverCert.pem
        rightauth=eap-radius
        rightsendcert=never
        eap_identity=%any
        compress=yes

conn PureIPSec
        keyexchange=ikev1
        aggressive=yes
        modeconfig=push
        dpdtimeout=1h
```

```
        dpddelay=300s
        dpdaction=clear
        auto=add
        rekey=no
        type=tunnel
        leftid=ipsec
        leftauth=psk
        rightauth=psk
        rightauth2=xauth-eap
        compress=yes

conn L2TP-PSK-noNAT
        #leftfirewall=yes
        #rightfirewall=yes
        keyexchange=ikev1
        dpdtimeout=1h
        dpddelay=300s
        dpdaction=clear
        auto=add
        rekey=no
        type=transport
        right=%any
        authby=psk
        leftprotoport=17/1701
        rightprotoport=17/%any
        compress=yes

conn IKEv2-1
        left=49.212.179.189
        leftsubnet=0.0.0.0/0
        right=%any
        rightsourceip=10.61.0.0/24
        also=PureIPSec-IKEv2

conn PureIPSec1
        left=49.212.179.189
        leftsubnet=0.0.0.0/0
        right=%any
        rightsourceip=10.60.0.0/24
        also=PureIPSec

conn L2TP-PSK-noNAT1
        left=49.212.179.189
        leftsubnet=0.0.0.0/0
        also=L2TP-PSK-noNAT

Feb 28 14:50:44 06[NET] received packet: from 60.166.119.217[53259] to 49.212.179.189[500] (1301 bytes)
Feb 28 14:50:44 06[ENC] parsed AGGRESSIVE request 0 [ SA KE No ID V V V V V V V V V V V V V ]
Feb 28 14:50:44 06[IKE] received XAuth vendor ID
Feb 28 14:50:44 06[IKE] received draft-ietf-ipsec-nat-t-ike-00 vendor ID
Feb 28 14:50:44 06[ENC] received unknown vendor ID: 16:f6:ca:16:e4:a4:06:6d:83:82:1a:0f:0a:ea:a8:62
Feb 28 14:50:44 06[IKE] received draft-ietf-ipsec-nat-t-ike-02\n vendor ID
Feb 28 14:50:44 06[IKE] received draft-ietf-ipsec-nat-t-ike-03 vendor ID
Feb 28 14:50:44 06[IKE] received NAT-T (RFC 3947) vendor ID
Feb 28 14:50:44 06[IKE] received FRAGMENTATION vendor ID
Feb 28 14:50:44 06[IKE] received DPD vendor ID
Feb 28 14:50:44 06[ENC] received unknown vendor ID: 3b:90:31:dc:e4:fc:f8:8b:48:9a:92:39:63:dd:0c:49
Feb 28 14:50:44 06[ENC] received unknown vendor ID: f1:4b:94:b7:bf:f1:fe:f0:27:73:b8:c4:9f:ed:ed:26
Feb 28 14:50:44 06[ENC] received unknown vendor ID: 16:6f:93:2d:55:eb:64:d8:e4:df:4f:d3:7e:23:13:f0:d0:fd:84:5
1
Feb 28 14:50:44 06[ENC] received unknown vendor ID: 84:04:ad:f9:cd:a0:57:60:b2:ca:29:2e:4b:ff:53:7b
Feb 28 14:50:44 06[IKE] received Cisco Unity vendor ID
Feb 28 14:50:44 06[IKE] 60.166.119.217 is initiating a Aggressive Mode IKE_SA
Feb 28 14:50:44 06[CFG] looking for XAuthInitPSK peer configs matching 49.212.179.189...60.166.119.217[ipsec]
Feb 28 14:50:44 06[CFG] selected peer config "PureIPSec1"
Feb 28 14:50:44 06[ENC] generating AGGRESSIVE response 0 [ SA KE No ID NAT-D NAT-D HASH V V V ]
Feb 28 14:50:44 06[NET] sending packet: from 49.212.179.189[500] to 60.166.119.217[53259] (521 bytes)
Feb 28 14:50:45 05[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (108 bytes)
Feb 28 14:50:45 05[ENC] parsed AGGRESSIVE request 0 [ HASH NAT-D NAT-D ]
Feb 28 14:50:45 05[IKE] local host is behind NAT, sending keep alives
Feb 28 14:50:45 05[IKE] remote host is behind NAT
Feb 28 14:50:45 05[ENC] generating TRANSACTION request 2973785907 [ HASH CPRQ(X_USER X_PWD) ]
Feb 28 14:50:45 05[NET] sending packet: from 49.212.179.189[4500] to 60.166.119.217[53260] (76 bytes)
Feb 28 14:50:45 04[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (92 bytes)
Feb 28 14:50:45 04[ENC] parsed INFORMATIONAL_V1 request 3485712151 [ HASH N(INITIAL_CONTACT) ]
```

```
Feb 28 14:50:45 12[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (92 bytes)
Feb 28 14:50:45 12[ENC] parsed TRANSACTION response 2973785907 [ HASH CPRP(X_TYPE X_USER X_PWD) ]
Feb 28 14:50:45 12[CFG] sending RADIUS Access-Request to server 'radius'
Feb 28 14:50:46 12[CFG] received RADIUS Access-Challenge from server 'radius'
Feb 28 14:50:46 12[CFG] sending RADIUS Access-Request to server 'radius'
Feb 28 14:50:46 12[CFG] received RADIUS Access-Challenge from server 'radius'
Feb 28 14:50:46 12[IKE] EAP-MS-CHAPv2 succeeded: '(null)'
Feb 28 14:50:46 12[CFG] sending RADIUS Access-Request to server 'radius'
Feb 28 14:50:46 12[CFG] received RADIUS Access-Accept from server 'radius'
Feb 28 14:50:46 12[CFG] scheduling RADIUS Interim-Updates every 300s
Feb 28 14:50:46 12[IKE] RADIUS authentication of 'wxm003' successful
Feb 28 14:50:46 12[IKE] XAuth authentication of 'wxm003' successful
Feb 28 14:50:46 12[ENC] generating TRANSACTION request 4006445755 [ HASH CPS(X_STATUS) ]
Feb 28 14:50:46 12[NET] sending packet: from 49.212.179.189[4500] to 60.166.119.217[53260] (76 bytes)
Feb 28 14:50:46 10[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (60 bytes)
Feb 28 14:50:46 10[ENC] parsed TRANSACTION response 4006445755 [ HASH CP ]
Feb 28 14:50:46 10[IKE] IKE_SA PureIPSec1[3200] established between 49.212.179.189[ipsec]...60.166.119.217[ips
ec]
Feb 28 14:50:46 10[CFG] assigning new lease to 'wxm003'
Feb 28 14:50:46 10[IKE] assigning virtual IP 10.60.0.69 to peer 'wxm003'
Feb 28 14:50:46 10[ENC] generating TRANSACTION request 3363496137 [ HASH CPS(ADDR DNS DNS) ]
Feb 28 14:50:46 10[NET] sending packet: from 49.212.179.189[4500] to 60.166.119.217[53260] (92 bytes)
Feb 28 14:50:46 13[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (92 bytes)
Feb 28 14:50:46 13[ENC] parsed TRANSACTION request 4006445755 [ HASH CPA(ADDR EXP MASK DNS NBNS SUBNET) ]
Feb 28 14:50:46 13[CFG] sending RADIUS Accounting-Request to server 'radius'
Feb 28 14:50:47 13[CFG] received RADIUS Accounting-Response from server 'radius'
Feb 28 14:50:47 13[ENC] generating TRANSACTION response 4006445755 [ HASH CP ]
Feb 28 14:50:47 13[NET] sending packet: from 49.212.179.189[4500] to 60.166.119.217[53260] (76 bytes)
Feb 28 14:51:05 08[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (92 bytes)
Feb 28 14:51:05 08[ENC] parsed INFORMATIONAL_V1 request 2758787308 [ HASH N(DPD) ]
Feb 28 14:51:10 10[IKE] sending keep alive to 60.166.119.217[53260]
Feb 28 14:51:25 13[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (92 bytes)
Feb 28 14:51:25 13[ENC] parsed INFORMATIONAL_V1 request 3334366065 [ HASH N(DPD) ]
Feb 28 14:51:30 14[IKE] sending keep alive to 60.166.119.217[53260]
Feb 28 14:51:35 07[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (1516 bytes)
Feb 28 14:51:35 07[ENC] parsed QUICK_MODE request 2174919514 [ HASH SA No ID ID ]
Feb 28 14:51:35 07[IKE] no matching CHILD_SA config found
Feb 28 14:51:36 15[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (92 bytes)
Feb 28 14:51:36 15[ENC] parsed INFORMATIONAL_V1 request 2744586831 [ HASH N(DPD) ]
Feb 28 14:51:39 11[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (92 bytes)
Feb 28 14:51:39 11[ENC] parsed INFORMATIONAL_V1 request 1986406884 [ HASH N(DPD) ]
Feb 28 14:51:43 05[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (1516 bytes)
Feb 28 14:51:43 05[ENC] invalid HASH_V1 payload length, decryption failed?
Feb 28 14:51:43 05[ENC] could not decrypt payloads
Feb 28 14:51:43 05[IKE] message parsing failed
Feb 28 14:51:43 05[ENC] generating INFORMATIONAL_V1 request 1984437889 [ HASH N(PLD_MAL) ]
Feb 28 14:51:43 05[NET] sending packet: from 49.212.179.189[4500] to 60.166.119.217[53260] (76 bytes)
Feb 28 14:51:43 05[IKE] QUICK_MODE request with message ID 2174919514 processing failed
Feb 28 14:51:43 04[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (92 bytes)
Feb 28 14:51:43 04[ENC] parsed INFORMATIONAL_V1 request 2625064681 [ HASH N(DPD) ]
Feb 28 14:51:50 08[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (1516 bytes)
Feb 28 14:51:50 08[ENC] invalid HASH_V1 payload length, decryption failed?
Feb 28 14:51:50 08[ENC] could not decrypt payloads
Feb 28 14:51:50 08[IKE] message parsing failed
Feb 28 14:51:50 08[ENC] generating INFORMATIONAL_V1 request 3040410051 [ HASH N(PLD_MAL) ]
Feb 28 14:51:50 08[NET] sending packet: from 49.212.179.189[4500] to 60.166.119.217[53260] (76 bytes)
Feb 28 14:51:50 08[IKE] QUICK_MODE request with message ID 2174919514 processing failed
Feb 28 14:51:55 10[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (1516 bytes)
Feb 28 14:51:55 10[ENC] invalid HASH_V1 payload length, decryption failed?
Feb 28 14:51:55 10[ENC] could not decrypt payloads
Feb 28 14:51:55 10[IKE] message parsing failed
Feb 28 14:51:55 10[ENC] generating INFORMATIONAL_V1 request 1559843057 [ HASH N(PLD_MAL) ]
Feb 28 14:51:55 10[NET] sending packet: from 49.212.179.189[4500] to 60.166.119.217[53260] (76 bytes)
Feb 28 14:51:55 10[IKE] QUICK_MODE request with message ID 2174919514 processing failed
Feb 28 14:51:59 09[NET] received packet: from 60.166.119.217[53260] to 49.212.179.189[4500] (92 bytes)
Feb 28 14:51:59 09[ENC] parsed INFORMATIONAL_V1 request 581087242 [ HASH D ]
Feb 28 14:51:59 09[IKE] received DELETE for IKE_SA PureIPSec1[3200]
Feb 28 14:51:59 09[IKE] deleting IKE_SA PureIPSec1[3200] between 49.212.179.189[ipsec]...60.166.119.217[ipsec]
```

#9 - 28.02.2014 08:42 - Tobias Brunner

- Status changed from Resolved to Closed

I'm closing this ticket, as the segfault is fixed. Please write to the mailing list if you still have configuration problems.

#10 - 05.06.2015 09:29 - Pavel Šimerda

We got a new related issue in Fedora caused by update from 5.2.0 to 5.2.2.

https://bugzilla.redhat.com/show_bug.cgi?id=1213650

#11 - 05.06.2015 10:32 - Tobias Brunner

@Pavel, I don't see how that issue is related (other than parts of the logs messages). This ticket here is about a crash! Your guy should check what's going on with the other peer and post more complete logs of both ends.