strongSwan - Bug #408
strongswan dies due to closeaction=restart
09.09.2013 23:26 - Noel Kuntze

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
<th>Start date:</th>
<th>09.09.2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td>Tobias Brunner</td>
<td>Estimated time:</td>
<td>0.00 hour</td>
</tr>
<tr>
<td>Category:</td>
<td>charon</td>
<td>Resolution:</td>
<td>Fixed</td>
</tr>
<tr>
<td>Target version:</td>
<td>5.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affected version:</td>
<td>5.1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description
On my box, charon is dieing. Sometimes with:

```
Sep 09 21:55:29 vms.thermi ipsec[228]: dumping 2 stack frame addresses:
Sep 09 21:55:29 vms.thermi ipsec[228]: /usr/lib/libpthread.so.0 @ 0x7f273ec96000 [0x7f273eca5870]
Sep 09 21:55:29 vms.thermi ipsec[228]: -> sigaction.c:?
Sep 09 21:55:29 vms.thermi ipsec[228]: [0x7f2704000078]
Sep 09 21:55:29 vms.thermi ipsec[228]: charon has died -- restart scheduled (5sec)
Sep 09 21:55:34 vms.thermi ipsec[228]: charon (9167) started after 80 ms
Sep 09 21:55:34 vms.thermi ipsec_starter[228]: charon (9167) started after 80 ms
```

And sometimes just with:

```
Sep 09 22:16:55 vms.thermi ipsec_starter[18431]: charon has died -- restart scheduled (5sec)
Sep 09 22:17:00 vms.thermi ipsec_starter[18431]: charon (21175) started after 120 ms
```

Linux kernel version is 3.10.10-1-ARCH and the distribution on both machines is Arch Linux. The client's and the server's logs are attached to the report.

How-to-cause:
(as client)

```
# ipsec start
# ipsec up server
# watch it trying to negotiate and crash
```

I could reproduce the issue 100% of times. It also crashes with "esp=aes256-sha256-ecp521!", which doesn't seem to be supported right now.

client:

```
# ipsec up server
initiating IKE_SA server[1] to 192.168.178.48
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) V ]
sending packet: from 192.168.178.43[500] to 192.168.178.48[500] (328 bytes)
received packet: from 192.168.178.48[500] to 192.168.178.43[500] (381 bytes)
parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
faking NAT situation to enforce UDP encapsulation
received cert request for "C=DE, ST=Baden-Württemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=ThermiCorp ServerCA Layer 2"
received cert request for "C=DE, ST=Baden-Württemberg, O=ThermiCorp, OU=ServerCA, CN=ThermiCorp UserCA Level 2"
received cert request for "C=DE, ST=Baden-Württemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=ThermiCorp Root CA, E=noel.kuntze@googlemail.com"
sending cert request for "C=DE, ST=Baden-Württemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=ThermiCorp User CA Level 2"
sending cert request for "C=DE, ST=Baden-Württemberg, L=Haslach, O=ThermiCorp, OU=Root CA, CN=ThermiCorp Root CA, E=noel.kuntze@googlemail.com"
```

19.03.2020
sending cert request for "C=DE, ST=Baden-Württemberg, O=ThermiCorp, OU=ServerCA Layer 2, CN=ThermiCorp ServerCA Layer 2"

authentication of 'nfs-client' (myself) with pre-shared key

establishing CHILD_SA server

generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ IDr AUTH N(ESP_TFC_PAD_N) SA TSi TSr N(MULT_AUTH) N(EAP_ONLY) ]
received packet: from 192.168.178.48[4500] to 192.168.178.43[4500] (240 bytes)
parsed IKE_AUTH response 1 [ IDr AUTH SA TSi TSr N(AUTH_LFT) ]

authentication of 'nfs-server' with pre-shared key successful
scheduling reauthentication in 9866s
maximum IKE_SA lifetime 10406s
can't install route for 192.168.178.43/32 === 192.168.178.48/32 out, conflicts with IKE traffic
unable to install IPsec policies (SPD) in kernel
failed to establish CHILD_SA, keeping IKE_SA
received AUTH_LIFETIME of 3369s, scheduling reauthentication in 2829s

sending DELETE for ESP CHILD_SA with SPI 59fa3d8f

generating INFORMATIONAL request 2 [ D ]
retransmit 1 of request with message ID 2
retransmit 2 of request with message ID 2

^C

ipsec.conf:

```
config setup
    # strictcrlpolicy=yes
    # uniqueids = no

conn %default
    leftupdown=/usr/lib/strongswan/sudo_updown

tc home
    auto=add
tc cacert=vpn-ca.pem

tc server
    auto=add
tc cacert=serverca.pem

tc user
    auto=add
tc cacert=userca.pem

tc server
    left=192.168.178.43
    leftid=nfs-client
    leftauth=psk
    ike=aes256-sha256-ecp521!
    esp=aes256-sha256-modp2048!
    keyexchange=ikev2
    rightauth=psk
    right=192.168.178.48
    rightid=nfs-server
    auto=add
    mobike=no

strongswan.conf:

    # strongswan.conf - strongSwan configuration file

charon {
    threads = 16
    send_vendor_id = yes
```
syslog {
    daemon {
        default=3
        enc=1
        job=1
        asn=1
        cfg=1
    }
}
filelog {
    /var/log/charon.log {
        default=3
        enc=1
        job=1
        asn=1
        cfg=1
    }
}
}

libstrongswan {
    dh_exponent_ansi_x9_42 = no
}

server:

journal output:

Sep 09 22:12:31 vms.thermi ipsec_starter[18422]: Starting strongSwan 5.1.0 IPsec [starter]...
Sep 09 22:12:31 vms.thermi ipsec_starter[18431]: charon (18432) started after 80 ms
Sep 09 22:16:55 vms.thermi ipsec_starter[18431]: charon has died -- restart scheduled (5sec)
Sep 09 22:17:00 vms.thermi ipsec_starter[18431]: charon (21175) started after 120 ms

ipsec.conf:

# ipsec.conf - strongSwan IPsec configuration file

# basic configuration
config setup
    uniqueids=replace
    strictcrlpolicy=no
ca home
    auto=add
    cacert=vpn-ca.pem
ca server
    auto=add
    cacert=serverca.pem
ca user
    auto=add
    cacert=userca.pem

conn %default
    ikelifetime=60m
    marginbytes=3000000000
    marginpackets=150000
    inactivity=0s
    keylife=20m
    rekeymargin=3m
    keyingtries=3
    tfc=%mtu
    dpdaction=restart
    dpddelay=10
    dpdtimeout=60
    compress=yes

19.03.2020
left=192.168.178.48
leftupdown=/usr/lib/strongswan/sudo_updown
(five connections redacted)
conn nfs
leftauth=psk
left=192.168.178.48
leftid=nfs-server
ike=aes256-sha256-ecp521!
esp=aes256-sha256-modp2048!
rightid=nfs-client
right=%any
rightauth=psk
auto=add
closeaction=restart

strongswan.conf:

# strongswan.conf - strongSwan configuration file

starter {
    load_warning = no
}

charon {
    load=charon test-vectors curl random nonce x509 revocation constraints pubkey pkcs1 pem op
    enssl af-alg gmp xcbc cmac hmac fips-pfr ccm attr kernel-netlink socket-default farp stroke updown
    eap-identity eap-gtc eap-mschapv2 eap-radius xauth-generic xauth-eap unity
    dns1=192.168.178.48
    dns2=192.168.178.6
    cisco_unity=yes
    threads = 32
    user=strongswan
    retry_initiate_interval = 3
    user=strongswan
    group=strongswan
    #
    # syslog {
    #    daemon {
    #        enc=-1
    #        cfg=1
    #        asn=1
    #        net=0
    #        ike=0
    #    }
    #
    #    }
    filelog {
        /var/log/charon.log {
            default = 3
            enc=2
            cfg=3
            asn=3
            append=no
            ike_name=no
        }
        /var/log/charon_compact.log {
            default = 3
            enc = 0
            cfg = 2
            asn = 1
            job = 1
            append=no
            ike_name=no
        }
        /var/log/charon_debug.log {
            default=3
        }
    }
libstrongswan {
    dh_exponent_ansi_x9_42 = yes
    crypto_test {
        bench=no
        bench_size=1500
        bench_time=50
        on_add=no
        required=no
    }
}

History

#1 - 10.09.2013 09:44 - Tobias Brunner
- Description updated
- Status changed from New to Resolved
- Assignee set to Tobias Brunner
- Target version set to 5.1.1
- Resolution set to Fixed

I think this is not due to the algorithms you chose but rather to a regression in 5.1.0 that broke closeaction=restart, which was already fixed with e42ab08a73.

#2 - 10.09.2013 16:25 - Tobias Brunner
- Status changed from Resolved to Closed

#3 - 01.11.2013 13:48 - Tobias Brunner
- Subject changed from strongswan dies with certain algorithms to strongswan dies due to closeaction=restart

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>charon_debug.log.tar.bz2</td>
<td>1.81 MB</td>
<td>09.09.2013</td>
<td>Noel Kuntze</td>
</tr>
<tr>
<td>charon.log</td>
<td>50.7 KB</td>
<td>09.09.2013</td>
<td>Noel Kuntze</td>
</tr>
</tbody>
</table>