

New issue

[Jump to bottom](#)

## xfrm interface ipsec1 exist after core dump and blocking restart of ipsec service clean #585

 Closed

MyOzCam opened this issue on Dec 21, 2021 · 4 comments

Labels

IKEv1

**MyOzCam** commented on Dec 21, 2021 • edited ▼

After setting up plutodebug=base, I got the packet which may cause core dump when ikev1 is not accept

```

Dec 21 02:43:35 localhost pluto[2787]: | *received 204 bytes from 101.4.62.36:43357 on eth0
192.168.99.102:500 using UDP
Dec 21 02:43:35 localhost pluto[2787]: | 31 27 fc b0 38 10 9e 89 00 00 00 00 00 00 00 1'..8.....
Dec 21 02:43:35 localhost pluto[2787]: | 01 10 02 00 00 00 00 00 00 00 00 cc 0d 00 00 5c .....
Dec 21 02:43:35 localhost pluto[2787]: | 00 00 00 01 00 00 00 01 00 00 00 50 01 01 00 02 .....P...
Dec 21 02:43:35 localhost pluto[2787]: | 03 00 00 24 01 01 00 00 80 01 00 05 80 02 00 02 ...$.
Dec 21 02:43:35 localhost pluto[2787]: | 80 04 00 02 80 03 00 03 80 0b 00 01 00 0c 00 04 .....
Dec 21 02:43:35 localhost pluto[2787]: | 00 00 0e 10 31 27 fc b0 38 10 9e 89 00 00 00 00 ....1'..8.....
Dec 21 02:43:35 localhost pluto[2787]: | 00 00 00 00 01 10 02 00 00 00 00 00 00 00 00 cc .....
Dec 21 02:43:35 localhost pluto[2787]: | 0d 00 00 5c 00 00 00 01 00 00 00 01 00 00 00 50 .....P
Dec 21 02:43:35 localhost pluto[2787]: | 01 01 00 02 03 00 00 24 01 01 00 00 80 01 00 05 .....$.
Dec 21 02:43:35 localhost pluto[2787]: | 80 02 00 02 80 04 00 02 80 03 00 03 80 0b 00 01 .....
Dec 21 02:43:35 localhost pluto[2787]: | 00 0c 00 04 00 00 0e 10 00 00 00 24 02 01 00 00 .....$.
Dec 21 02:43:35 localhost pluto[2787]: | 80 01 00 05 80 02 00 01 80 04 00 02 80 03 00 03 .....
Dec 21 02:43:35 localhost pluto[2787]: | 80 0b 00 01 00 0c 00 04 00 00 0e 10 .....
Dec 21 02:43:35 localhost pluto[2787]: | **parse ISAKMP Message:
Dec 21 02:43:35 localhost pluto[2787]: | initiator SPI: 31 27 fc b0 38 10 9e 89
Dec 21 02:43:35 localhost pluto[2787]: | responder SPI: 00 00 00 00 00 00 00 00
Dec 21 02:43:35 localhost pluto[2787]: | next payload type: ISAKMP_NEXT_SA (0x1)
Dec 21 02:43:35 localhost pluto[2787]: | ISAKMP version: ISAKMP Version 1.0 (rfc2407) (0x10)
Dec 21 02:43:35 localhost pluto[2787]: | exchange type: ISAKMP_XCHG_IDPROT (0x2)
Dec 21 02:43:35 localhost pluto[2787]: | flags: none (0x0)
Dec 21 02:43:35 localhost pluto[2787]: | Message ID: 0 (00 00 00 00)
Dec 21 02:43:35 localhost pluto[2787]: | length: 204 (00 00 00 cc)
Dec 21 02:43:35 localhost pluto[2787]: | processing version=1.0 packet with exchange
type=ISAKMP_XCHG_IDPROT (2)
Dec 21 02:43:35 localhost pluto[2787]: | State DB: IKEv1 state not found (find_state_ikev1_init)
Dec 21 02:43:35 localhost pluto[2787]: | #null state always idle
Dec 21 02:43:35 localhost pluto[2787]: | got payload 0x2 (ISAKMP_NEXT_SA) needed: 0x2 opt: 0x2080
Dec 21 02:43:35 localhost pluto[2787]: | ***parse ISAKMP Security Association Payload:
Dec 21 02:43:35 localhost pluto[2787]: | next payload type: ISAKMP_NEXT_VID (0xd)
Dec 21 02:43:35 localhost pluto[2787]: | length: 92 (00 5c)
Dec 21 02:43:35 localhost pluto[2787]: | DOI: ISAKMP_DOI_IPSEC (0x1)
Dec 21 02:43:35 localhost pluto[2787]: | got payload 0x2000 (ISAKMP_NEXT_VID) needed: 0x0 opt: 0x2080
Dec 21 02:43:36 localhost systemd[1]: ipsec.service: Main process exited, code=dumped, status=11/SEGV
Dec 21 02:43:36 localhost systemd[1]: ipsec.service: Failed with result 'core-dump'.
Dec 21 02:43:36 localhost systemd[1]: ipsec.service: Consumed 2.706s CPU time.
Dec 21 02:43:36 localhost systemd[1]: ipsec.service: Scheduled restart job, restart counter is at 2.
Dec 21 02:43:36 localhost systemd[1]: Stopped Internet Key Exchange (IKE) Protocol Daemon for IPsec.
Dec 21 02:43:36 localhost systemd[1]: ipsec.service: Consumed 2.706s CPU time.
Dec 21 02:43:36 localhost systemd[1]: Starting Internet Key Exchange (IKE) Protocol Daemon for IPsec...

```

normally after core dump the IPsec service restart but unfortunately the original xfrm interface was not clear and cause below:

*Dec 21 02:43:38 localhost pluto[3815]: "ikev2-cp": conflict ipsec1 already exist cannot support xfrm-interface.  
May be leftover from previous pluto?*

*Dec 21 02:43:38 localhost pluto[3815]: "ikev2-cp": failed to add connection: ipsec-interface=1 not supported.  
device name conflict in xfrm\_iface\_supported()*

This cause the VPN server not accept any connection request and need manual restart the service.

Any workaround?

**paulwouters** commented on Dec 21, 2021

Member

thanks for capturing the full packet. I replayed it in my test setup but it did not crash. Can you give me your /etc/ipsec.conf and any included conf files so I can fully reproduce your setup?

Dec 21 18:08:21.770741: | \*received 204 bytes from 192.1.2.45:48730 on eth1 192.1.2.23:500 using UDP  
Dec 21 18:08:21.770778: | 31 27 fc b0 38 10 9e 89 00 00 00 00 00 00 00 00 1'..8.....  
Dec 21 18:08:21.770810: | 01 10 02 00 00 00 00 00 00 00 00 00 cc 0d 00 00 5c .....  
Dec 21 18:08:21.770840: | 00 00 00 01 00 00 00 01 00 00 00 50 01 01 00 02 .....P...  
Dec 21 18:08:21.770870: | 03 00 00 24 01 01 00 00 80 01 00 05 80 02 00 02 ...\$.  
Dec 21 18:08:21.770900: | 80 04 00 02 80 03 00 03 80 0b 00 01 00 0c 00 04 .....  
Dec 21 18:08:21.770944: | 00 00 0e 10 31 27 fc b0 38 10 9e 89 00 00 00 00 ....1'..8.....  
Dec 21 18:08:21.770976: | 00 00 00 00 01 10 02 00 00 00 00 00 00 00 00 cc .....  
Dec 21 18:08:21.771006: | 0d 00 00 5c 00 00 00 01 00 00 00 01 00 00 00 50 .....P  
Dec 21 18:08:21.771034: | 01 01 00 02 03 00 00 24 01 01 00 00 80 01 00 05 .....\$.  
Dec 21 18:08:21.771089: | 80 02 00 02 80 04 00 02 80 03 00 03 80 0b 00 01 .....  
Dec 21 18:08:21.771118: | 00 0c 00 04 00 00 0e 10 00 00 00 24 02 01 00 00 .....\$.  
Dec 21 18:08:21.771147: | 80 01 00 05 80 02 00 01 80 04 00 02 80 03 00 03 .....  
Dec 21 18:08:21.771179: | 80 0b 00 01 00 0c 00 04 00 00 0e 10 .....  
Dec 21 18:08:21.771210: | \*\*parse ISAKMP Message:  
Dec 21 18:08:21.771238: | initiator SPI: 31 27 fc b0 38 10 9e 89  
Dec 21 18:08:21.771268: | responder SPI: 00 00 00 00 00 00 00 00  
Dec 21 18:08:21.771350: | next payload type: ISAKMP\_NEXT\_SA (0x1)  
Dec 21 18:08:21.771435: | ISAKMP version: ISAKMP Version 1.0 (rfc2407) (0x10)  
Dec 21 18:08:21.771459: | exchange type: ISAKMP\_XCHG\_IDPROT (0x2)  
Dec 21 18:08:21.771487: | flags: none (0x0)  
Dec 21 18:08:21.771514: | Message ID: 0 (00 00 00 00)  
Dec 21 18:08:21.771542: | length: 204 (00 00 00 cc)  
Dec 21 18:08:21.771571: | processing version=1.0 packet with exchange type=ISAKMP\_XCHG\_IDPROT (2)  
Dec 21 18:08:21.771601: | State DB: IKEv1 state not found (find\_state\_ikev1\_init)  
Dec 21 18:08:21.771626: | #null state always idle  
Dec 21 18:08:21.771654: | got payload 0x2 (ISAKMP\_NEXT\_SA) needed: 0x2 opt: 0x2080  
Dec 21 18:08:21.771683: | \*\*\*parse ISAKMP Security Association Payload:  
Dec 21 18:08:21.771720: | next payload type: ISAKMP\_NEXT\_VID (0xd)  
Dec 21 18:08:21.771744: | length: 92 (00 5c)  
Dec 21 18:08:21.771772: | DOI: ISAKMP\_DOI\_IPSEC (0x1)  
Dec 21 18:08:21.771799: | got payload 0x2000 (ISAKMP\_NEXT\_VID) needed: 0x0 opt: 0x2080  
Dec 21 18:08:21.771831: packet from 192.1.2.45:48730: 1-byte length of ISAKMP Vendor ID Payload is smaller than minimum  
Dec 21 18:08:21.771861: packet from 192.1.2.45:48730: malformed payload in packet  
Dec 21 18:08:21.771892: | delref struct msg\_digest@0x55f7409eb7f8(1->0) (process\_iface\_packet() +305 programs/pluto/demux.c)  
Dec 21 18:08:21.771920: | delref logger@0x55f7409d9898(1->0) (process\_iface\_packet() +305 programs/pluto/demux.c)  
Dec 21 18:08:21.771944: | delref fd@NULL (process\_iface\_packet() +305 programs/pluto/demux.c)  
Dec 21 18:08:21.771971: | delref fd@NULL (process\_iface\_packet() +305 programs/pluto/demux.c)  
Dec 21 18:08:21.771998: | delref struct iface\_endpoint@0x55f7409eab38(4->3) (process\_iface\_packet() +305 programs/pluto/demux.c)  
Dec 21 18:08:21.772030: | spent 0.402 (1.69) milliseconds in process\_iface\_packet() reading and processing packet  
Dec 21 18:08:22.806161: | processing global timer EVENT\_PENDING\_DDNS

Dec 21 18:08:22.806475: | FOR\_EACH\_CONNECTION\_.... in (connection\_check\_ddns() +1184  
programs/pluto/initiate.c)  
Dec 21 18:08:22.806629: | found "ikev2"  
Dec 21 18:08:22.806733: | found "ikev1"  
Dec 21 18:08:22.806900: | matches: 2  
Dec 21 18:08:22.807010: | FOR\_EACH\_UNORIENTED\_CONNECTION\_... in check\_orientations  
Dec 21 18:08:22.807122: | spent 0.115 (0.642) milliseconds in in connection\_check\_ddns for hostname lookup  
Dec 21 18:08:22.807210: | spent 0.145 (0.738) milliseconds in global timer EVENT\_PENDING\_DDNS  
Dec 21 18:08:22.825421: | processing global timer EVENT\_SHUNT\_SCAN  
Dec 21 18:08:22.825605: | kernel: checking for aged bare shunts from shunt table to expire  
Dec 21 18:08:22.825736: | spent 0.0245 (0.126) milliseconds in global timer EVENT\_SHUNT\_SCAN  
Dec 21 18:08:42.834790: | processing global timer EVENT\_SHUNT\_SCAN  
Dec 21 18:08:42.835056: | kernel: checking for aged bare shunts from shunt table to expire  
Dec 21 18:08:42.835140: | spent 0.0178 (0.0808) milliseconds in global timer EVENT\_SHUNT\_SCAN  
Dec 21 18:09:02.836858: | processing global timer EVENT\_SHUNT\_SCAN  
Dec 21 18:09:02.837147: | kernel: checking for aged bare shunts from shunt table to expire  
Dec 21 18:09:02.837401: | spent 0.0347 (0.249) milliseconds in global timer EVENT\_SHUNT\_SCAN  
Dec 21 18:09:02.837572: | processing global timer EVENT\_SD\_WATCHDOG  
Dec 21 18:09:02.837735: | pluto\_sd: executing action action: watchdog(3), status 0  
Dec 21 18:09:02.837987: | spent 0.143 (0.251) milliseconds in global timer EVENT\_SD\_WATCHDOG  
Dec 21 18:09:22.825274: | processing global timer EVENT\_PENDING\_DDNS  
Dec 21 18:09:22.825420: | FOR\_EACH\_CONNECTION\_.... in (connection\_check\_ddns() +1184  
programs/pluto/initiate.c)  
Dec 21 18:09:22.825599: | found "ikev2"  
Dec 21 18:09:22.825665: | found "ikev1"  
Dec 21 18:09:22.825732: | matches: 2  
Dec 21 18:09:22.825785: | FOR\_EACH\_UNORIENTED\_CONNECTION\_... in check\_orientations  
Dec 21 18:09:22.825906: | spent 0.0695 (0.483) milliseconds in in connection\_check\_ddns for hostname  
lookup  
Dec 21 18:09:22.825942: | spent 0.0879 (0.524) milliseconds in global timer EVENT\_PENDING\_DDNS  
Dec 21 18:09:22.825980: | processing global timer EVENT\_PENDING\_PHASE2  
Dec 21 18:09:22.826014: | FOR\_EACH\_CONNECTION\_.... in (connection\_check\_phase2() +1203  
programs/pluto/initiate.c)  
Dec 21 18:09:22.826048: | found "ikev2"  
Dec 21 18:09:22.826081: | pending review: connection "ikev2" was not up, skipped  
Dec 21 18:09:22.826114: | found "ikev1"  
Dec 21 18:09:22.826145: | pending review: connection "ikev1" was not up, skipped  
Dec 21 18:09:22.826172: | matches: 2  
Dec 21 18:09:22.826210: | spent 0.0373 (0.197) milliseconds in global timer EVENT\_PENDING\_PHASE2  
Dec 21 18:09:22.826241: | processing global timer EVENT\_SHUNT\_SCAN  
Dec 21 18:09:22.826266: | kernel: checking for aged bare shunts from shunt table to expire  
Dec 21 18:09:22.826296: | spent 0.00767 (0.0296) milliseconds in global timer EVENT\_SHUNT\_SCAN

Never mind. Cagney already fixed it. I can confirm the packet you captured causes a crash in libreswan 4.2 - 4.5

  **letoams** added the `IKEv1` label on Dec 22, 2021

**MyOzCam** commented on Dec 22, 2021

Author

That is correct. Thanks **@cagney** and the team.

When will release 4.6 which may incorporate this fix?

 **letoams** commented on Dec 23, 2021

Member

On Wed, 22 Dec 2021, MyOzCam wrote:


That is correct. Thanks **@cagney** and the team.

When will release 4.6 which may incorporate this fix?

January 5.

If you want something sooner try:

```
git clone github.com/libreswan/libreswan
cd libreswan
make rpm
```

 **MyOzCam** closed this as completed on Aug 24

---

#### Assignees

No one assigned

---

#### Labels

`IKEv1`

---

#### Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

3 participants

