strongSwan - Bug #3391

Strongswan complitelly crashes and restarts itself.

01.04.2020 02:22 - Darko Kraus

Status:	Closed	Start date:	01.04.2020
Priority:	Normal	Due date:	
Assignee:	Tobias Brunner	Estimated time:	0.00 hour
Category:	ikev1		
Target version:	5.8.4		
Affected version:	5.8.3	Resolution:	Fixed

Description
Hello,

I believe I have discovered a serious bug where strongswan / ipsec daemon crashes, drops all the connections and restarts itself.

Here is little history... I am using strongswan for a server that accepts multiple connections from TP-Link R600VPN routers and everything works fine. However I was testing Linksys router model LRT214, and when that router attempts to make the connection to my linux server, after about 30 seconds of failed negotiations, the ipsec daemon crashes and restarts itself. Of course that drops all existing ipsec tunnels. I have tested this scenario on 2 different linux machines, one with linux kernel 3.16.82 and the other with linux kernel 4.4.14 and got the same results.

I have included the log file, ipsec.conf and ipsec.secrets. If you need any additional info or want me to point the Linksys VPN routers to one of your servers so you can capture what exactly it sends please let me know. The current debug level is set to default which is 1.

Thank you again for your help!

History

#1 - 01.04.2020 04:29 - Darko Kraus

- File charonlog-level2 added

I attached more detailed log with level=2.

Also I wanted to add, when you type ipsec status you get...

root@FWJUPITER:/etc# ipsec status
Security Associations (2 up, 0 connecting):
GW-REMUSR45[2]: ESTABLISHED 5 seconds ago, 172.16.95.30[FWJUPITER.domain1.org]
...50.50.50.50[GW-REMUSR45.domain1.org]
GW-REMUSR45[1]: ESTABLISHED 35 seconds ago, 172.16.95.30[FWJUPITER.domain1.org
]...50.50.50.50[GW-REMUSR45.domain1.org]

The tunnel never gets established, but it creates multiple entries of the IKE? First there was only one, then when I typed ipsec status again, I got 2 entries.

Thanks,
Darko

#2 - 01.04.2020 09:12 - Tobias Brunner

- Category set to ikev1

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Priority changed from Urgent to Normal

- Target version set to 5.8.4

- Resolution set to Fixed

The crash has already been fixed with 5.8.4.

The reason it got triggered here is because your ESP proposals don't match (the initiator want's to use PFS, i.e. proposes a DH group, the responder

doesn't).

#3 - 01.04.2020 22:35 - Darko Kraus

Hi Tobias,

Just wanted to give you an update. Appears that version 5.8.2 was not affected by this bug. This bug exists only in 5.8.3 version. I have tested 5.8.2, 5.8.3 and 5.8.4 where 5.8.2 and 5.8.4 work fine and 5.8.3 is the only one that crashes. Thank you for a quick update!

#4 - 02.04.2020 10:44 - Tobias Brunner

> Appears that version 5.8.2 was not affected by this bug. This bug exists only in 5.8.3 version.

Yes, it was a bug in changes for [5.8.3](#) hence the [5.8.4](#) release only a week later (also see [the announcement in our blog](#)).

Files

ipsec.conf	816 Bytes	01.04.2020	Darko Kraus
charonlog	11.6 KB	01.04.2020	Darko Kraus
ipsec.secrets	251 Bytes	01.04.2020	Darko Kraus
charonlog-level2	139 KB	01.04.2020	Darko Kraus