strongSwan - Issue #2894

Ubuntu strongswan-nm plugin not using server assigned DNS servers

23.01.2019 22:27 - James Dogopoulos

Status:	Closed			
Priority:	Normal			
Assignee:	Tobias Brunner			
Category:	networkmanager (charon-nm)			
Affected version:	5.6.2	**Resolution:**	No change required	

Description

This is another security/privacy issue, DNS resolution still seems to go out of the client's wifi/ethernet instead of using the DNS resolvers pushed by the server.

This is an issue with Windows clients as well but I may be opening separate issue for that soon once I look into it more.

History

#1 - 23.01.2019 23:04 - James Dogopoulos

I tried disabling systemd-resolvd per [[https://askubuntu.com/questions/907246/how-to-disable-systemd-resolved-in-ubuntu]] which solves DNS leak issues for openvpn but now name server being written to for strongswan are as follows:

```
root@jd:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 0.71.1.56
nameserver 16.62.1.56
```

No idea where it got these from

#2 - 24.01.2019 09:32 - Tobias Brunner

- Status changed from New to Feedback

What version are you actually using? There was a bug in 5.6.2 that was subsequently fixed with 5.6.3 (ee8c25516a), which caused invalid DNS servers to be configured via NM.

Also, fixing that DNS leak issue without disabling systemd-resolved requires very current versions of NM and/or systemd-resolved (just search the systemd issue tracker).

#3 - 24.01.2019 16:09 - James Dogopoulos

Yup, you got it, it's an old strongSwan, I saw a strongswan update on Ubuntu 18 but it was just some minor revisions and they aren't updating to latest code. **sobs**   AND looks like the DNS leak issue is finally fixed in a proposed systemd update but hasn't made it into mainline code just yet.

So I guess the only thing left is the nm plugin IPv6 issue.

#4 - 25.01.2019 08:51 - Tobias Brunner

- Category set to networkmanager (charon-nm)

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Affected version changed from 5.7.2 to 5.6.2

- Resolution set to No change required