strongSwan - Bug #780

Default _updown script is logging IP address to syslog

01.12.2014 18:07 - Lian Duan

Status:	Closed	**Start date:**	01.12.2014
Priority:	Normal	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.2.2		
Affected version:	5.2.1	**Resolution:**	Fixed

Description

We found logs with sensitive client information(IP address) in our servers' syslog after we have explicitly setting all logging levels to -1.

HOSTNAME vpn: - CLIENT_ID VIRTUAL_IP/32 CLIENT_IP -- SERVER_IP 0.0.0.0/0

It turns out to be the default _updown script is sending this log line to syslog.

In src/_updown/_updown.in,

```
131 # uncomment to log VPN connections
132    VPN_LOGGING=1
133    #
```

Line 132 should be commented out by default, as also stated by the comment.

Associated revisions

Revision dcae0a39 - 02.12.2014 15:02 - Martin Willi

updown: Inverse comment of VPN_LOGGING variable, as it is enabled by default

Fixes #780.

History

#1 - 02.12.2014 14:52 - Martin Willi

- Status changed from New to Feedback

Hi,

Yes, this is the default behavior when the updown script is used, and it has been ever since (at least with charon).

I'd like to avoid changing that default behavior, as some installations might rely on it. We certainly can improve the documentation, which I've tried to address with the new updown Wiki page.

Regards
Martin

#2 - 02.12.2014 15:04 - Martin Willi

The associated commit fixes the comment in the default updown script.

#3 - 19.12.2014 14:15 - Martin Willi

- Tracker changed from Issue to Bug

- Category set to libcharon

- Status changed from Feedback to Closed

- Target version set to 5.2.2

- Resolution set to Fixed