strongSwan - Bug #1138

ext-auth plugin not called when using xauth-noauth

29.09.2015 17:00 - Alexey Karagodov

Status:	Closed	**Start date:**	29.09.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.4		
Affected version:	5.3.3	**Resolution:**	Fixed

Description

hello

ext-auth plugin does nothing

only line in logs: "charon: 00[CFG] using ext-auth script '/usr/local/etc/ipsec.d/connect.sh'"

when someone trying to connect to host, script is not called at all.

strongswan 5.3.3 build from freebsd-port with options --enable-xauth-noauth --enable-ext-auth

please, help.

thanx

Associated revisions

Revision bd5084ae - 09.11.2015 14:44 - Tobias Brunner

xauth: Call authorize() hook also when xauth-noauth is used

Fixes #1138.

History

#1 - 30.09.2015 01:41 - Noel Kuntze

Hello,

Is the user you're running charon as allowed to reach and execute the script? Is a security framework enabled?

Regards,
Noel Kuntze

#2 - 30.09.2015 07:30 - Alexey Karagodov

running under root, for testing.

5 -rwxr-xr-x 1 root wheel 813 Sep 29 15:54 /usr/local/etc/ipsec.d/connect.sh

no security frameworks active.

in the journal no reports that charon tries to run a script ...

#3 - 01.10.2015 15:00 - Tobias Brunner

- Status changed from New to Feedback

> charon: 00[CFG] using ext-auth script '/usr/local/etc/ipsec.d/connect.sh'

That's logged when the plugins loads the config.

In the authorize hook the plugin tries to invoke (via fork/execve) /bin/sh -c "2>&1 /usr/local/etc/ipsec.d/connect.sh", which I guess should work fine on

FreeBSD. At least if the authorize hook is called. Could you please post the log of a connection attempt.

#4 - 01.10.2015 15:19 - Alexey Karagodov

> In the authorize hook the plugin tries to invoke (via fork/execve) /bin/sh -c "2>&1 /usr/local/etc/ipsec.d/connect.sh", which I guess should work fine on FreeBSD. At least if the authorize hook is called. Could you please post the log of a connection attempt.

how to do it w/o logging sensitive data?

#5 - 01.10.2015 15:22 - Alexey Karagodov

- File strongswan.log added

#6 - 05.10.2015 17:53 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from ext-auth plugin to ext-auth plugin not called when using xauth-noauth

- Target version set to 5.3.4

Looks like this is due to the *xauth-noauth* plugin (which is a hack and really should only be used in special circumstances). It takes a shortcut in the *xauth* task, which does not call the authorize hook. You may try the patch in the *1138-xauth-noauth-authorize* branch to change this.

Also, there seem to be log messages missing here:

```
2015-10-01T16:20:58+03:00 s_client@probe0226.domain.tld charon: 05[MGR] checkout IKE_SA by message
2015-10-01T16:20:58+03:00 s_client@probe0226.domain.tld charon: 05[MGR] IKE_SA CiscoIPSec[1] successfully
checked out
2015-10-01T16:20:58+03:00 s_client@probe0226.domain.tld charon: 05[NET] received packet: from 109.188.127.
12[36970] to 10.0.226.60[4500] (76 bytes)
...
2015-10-01T16:20:58+03:00 s_client@probe0226.domain.tld charon: 05[ENC] parsed TRANSACTION response 114209
4431 [ HASH CPA(X_STATUS) ]
```

We don't see thread 5 checking in the SA again but thread 12 is still able to checkout the SA right afterwards:

```
2015-10-01T16:20:58+03:00 s_client@probe0226.domain.tld charon: 12[MGR] IKE_SA CiscoIPSec[1] successfully
checked out
2015-10-01T16:20:58+03:00 s_client@probe0226.domain.tld charon: 12[MGR] checkin IKE_SA CiscoIPSec[1]
```

We also don't see the message IKE_SA ... established between ... that should have been logged by thread 5.

#7 - 06.10.2015 00:21 - Alexey Karagodov

where can i find this patch?
or target version sources?

#8 - 06.10.2015 00:35 - Noel Kuntze

Hi Alexey,

Here's a link to the patch:
https://wiki.strongswan.org/projects/strongswan/repository/diff?utf8=%E2%9C%93&rev=92e9b1d18bac1cfc004c96e60d5bc7f3a0428f70&rev_to=08afc33e5259399a682bb62ef253b3155e68461e
This is the associated commit. Download the patch by downloading the unified patch and patch the source of 5.3.3 with it.

#9 - 06.10.2015 13:38 - Alexey Karagodov

thanx. building. 'll report.

#10 - 06.10.2015 14:05 - Alexey Karagodov

patch helped.
ext-auth + xauth-noauth are working now.

your patch was modified (to match freebsd port's point of view) and applied to freebsd port

#11 - 06.10.2015 14:37 - Alexey Karagodov

- File patch-src_libcharon_sa_ikev1_tasks_xauth.c added

- File Makefile.local added

#12 - 06.10.2015 15:04 - Tobias Brunner

- Category set to libcharon

- Status changed from Feedback to Resolved

- Assignee set to Tobias Brunner

- Resolution set to Fixed

OK, thanks for testing. I'll line this up for the next release.

#13 - 09.11.2015 15:03 - Tobias Brunner

- Status changed from Resolved to Closed

Files

strongswan.log	803 KB	01.10.2015	Alexey Karagodov
patch-src_libcharon_sa_ikev1_tasks_xauth.c	1019 Bytes	06.10.2015	Alexey Karagodov
Makefile.local	606 Bytes	06.10.2015	Alexey Karagodov