strongSwan - Feature #264

IKE message fragmentation (cisco) + IOS 6.0 Hack for encrypted flaged ike fragmentation packets

13.12.2012 10:22 - Daniel Danzberger

Status:	Closed	**Start date:**	13.12.2012
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.0.2		
Resolution:	Fixed		

Description

Hi,

since Apple's IOS 6 we noticed, that some clients send bigger IKE messages in fragments. They use the proprietary undocumented cisco IKE fragmentation protocol.
So we thought it would be nice if strongswan can support it. There is a patch from astaro for version 4.x.x . But none for 5.0.1 yet.

----
src/libcharon/Makefile.am | 2
src/libcharon/Makefile.in | 38 ++-
src/libcharon/daemon.c | 2
src/libcharon/daemon.h | 6 +
src/libcharon/encoding/message.c | 35 ++
src/libcharon/encoding/message_fragmentation.c | 372 +++++++++++++++++++++++++++++
src/libcharon/encoding/message_fragmentation.h | 26 ++
src/libcharon/encoding/payloads/cisco_ikefrag_payload.c | 165 +++++++++++++
src/libcharon/encoding/payloads/cisco_ikefrag_payload.h | 32 ++
src/libcharon/encoding/payloads/payload.c | 9 +
src/libcharon/encoding/payloads/payload.h | 2 +
src/libcharon/network/receiver.c | 68 ++--
src/libcharon/network/receiver.h | 6 +

This little patch works for us. Tested with the shrew client on windows 7 and some IOS Apple devices.
Beside the fragmentation code, it also involves a little hack for IOS devices that (wrongly) send fragmented packets with the encrypted flag set,
even if the content is not encrypted.

We are currently working on adding this feature to the sa_payload's proposals.

Related issues:

Related to Feature #115: Does pluto support Vendor ID payload with "IKE Fragm...	**Closed**	**27.07.2010**

History

#1 - 13.12.2012 10:36 - Tobias Brunner

- Status changed from New to Feedback

Thank's for the patch.

I've actually been working on this myself. You can check the ikev1-fragments branch of our repository.

#2 - 14.12.2012 11:11 - Tobias Brunner

- Category set to charon

- Status changed from Feedback to Assigned

- Assignee set to Tobias Brunner

- Target version set to 5.0.2

#3 - 24.12.2012 13:33 - Azfar Hashmi

I am applying this patch on strongswan_4.5.2 (Debian) but it is failing.

patching file src/libcharon/Makefile.am
Hunk #1 succeeded at 14 (offset ~~1 lines).~~
~~Hunk #2 succeeded at 28 (offset -1 lines).~~
~~patching file src/libcharon/Makefile.in~~
~~Hunk #1 succeeded at 603 (offset 328 lines).~~
~~Hunk #2 succeeded at 624 (offset 328 lines).~~
~~Hunk #3 FAILED at 443.~~
~~Hunk #4 FAILED at 731.~~
~~Hunk #5 succeeded at 626 (offset -125 lines).~~
~~Hunk #6 succeeded at 879 (offset -111 lines).~~
~~Hunk #7 succeeded at 926 with fuzz 2 (offset -123 lines).~~
~~Hunk #8 succeeded at 1064 (offset -132 lines).~~
~~Hunk #9 succeeded at 1162 (offset -132 lines).~~
~~2 out of 9 hunks FAILED~~ saving rejects to file src/libcharon/Makefile.in.rej
patching file src/libcharon/daemon.c
Hunk #1 FAILED at 119.
Hunk #2 FAILED at 237.
2 out of 2 hunks FAILED -- saving rejects to file src/libcharon/daemon.c.rej
patching file src/libcharon/daemon.h
Hunk #1 FAILED at 166.
Hunk #2 succeeded at 253 with fuzz 2 (offset ~~19 lines).~~
~~1 out of 2 hunks FAILED~~ saving rejects to file src/libcharon/daemon.h.rej
patching file src/libcharon/encoding/message.c
Hunk #2 succeeded at 35 with fuzz 1.
Hunk #3 succeeded at 549 (offset ~~325 lines).~~
~~Hunk #4 FAILED at 1736.~~
~~Hunk #5 succeeded at 1287 with fuzz 1 (offset -507 lines).~~
~~Hunk #6 FAILED at 1816.~~
~~Hunk #7 FAILED at 1985.~~
~~Hunk #8 FAILED at 2009.~~
~~Hunk #9 succeeded at 1503 (offset -568 lines).~~
~~4 out of 9 hunks FAILED~~ saving rejects to file src/libcharon/encoding/message.c.rej
patching file src/libcharon/encoding/message_fragmentation.c
patching file src/libcharon/encoding/message_fragmentation.h
patching file src/libcharon/encoding/payloads/cisco_ikefrag_payload.c
patching file src/libcharon/encoding/payloads/cisco_ikefrag_payload.h
patching file src/libcharon/encoding/payloads/payload.c
Hunk #1 succeeded at 35 with fuzz 2 (offset ~~2 lines).~~
~~Hunk #2 FAILED at 55.~~
~~Hunk #3 FAILED at 81.~~
~~Hunk #4 FAILED at 94.~~
~~Hunk #5 FAILED at 165.~~
~~Hunk #6 FAILED at 252.~~
~~5 out of 6 hunks FAILED~~ saving rejects to file src/libcharon/encoding/payloads/payload.c.rej
patching file src/libcharon/encoding/payloads/payload.h
Hunk #1 succeeded at 131 (offset ~~89 lines).~~
~~patching file src/libcharon/network/receiver.c~~
~~Hunk #1 FAILED at 407.~~
~~Hunk #2 FAILED at 440.~~
~~Hunk #3 FAILED at 448.~~
~~Hunk #4 FAILED at 466.~~
~~Hunk #5 FAILED at 580.~~
~~Hunk #6 succeeded at 373 with fuzz 1 (offset -228 lines).~~
~~Hunk #7 FAILED at 623.~~
~~6 out of 7 hunks FAILED~~ saving rejects to file src/libcharon/network/receiver.c.rej
patching file src/libcharon/network/receiver.h
Hunk #1 succeeded at 52 with fuzz 1 (offset -32 lines).

tried it on 4.4.1-5.2 and 4.6.4 (latest source) but failing on them too.

For which 4.x.x version it is tested/for? I need to apply it on stock debain strongswan source.

#4 - 24.12.2012 13:40 - Daniel Danzberger

hi,

this patch is for 5.0.1.
here is the source is used -> http://download.strongswan.org/strongswan-5.0.1.tar.bz2

#5 - 24.12.2012 13:50 - Christian Scheele

Hi,

for 4.4.x, 4.5.x or 4.6.x you need the astaro patch, that you can get in the big-iso sourcecode download from astaro, or here:

http://pastebin.com/mHS68juq

See this discussion for little further info.

http://comments.gmane.org/gmane.network.vpn.strongswan.user/5597

#6 - 26.12.2012 17:04 - Azfar Hashmi

Thanks Daniel and Christian. I have one more question. Is this patch/workaround has any relation with various iOS 6 versions for example 6.0, 6.0.1, 6.0.2, 6.1 beta etc?

#7 - 30.12.2012 10:52 - Christian Scheele

Hi,

i just quote from the Astaro patch description:

> The IPsec client in iOS 6 sends IKE packets split up into
> IKE fragment payloads in some situations. This is done
> regardless of whether UTM announces support for this
> undocumented Cisco proprietary IKE extension or not.
>
> This patch adds support for incoming IKE fragments.

==> without that -> connection not possible.

This behavior applies to iOS 6.0 6.0.1 6.0.2.

iOS 6.1.b3+b4 is already fixed by apple, so i would bet that the upcoming ios 6.1 will not need this patch.

#8 - 12.01.2013 12:05 - Tobias Brunner

- Status changed from Assigned to Resolved

- Resolution set to Fixed

This is now implemented in master and will be included in the upcoming 5.0.2 release.

#9 - 21.01.2013 17:26 - Tobias Brunner

- Status changed from Resolved to Closed

Files

ikefrag.patch	35.5 KB	13.12.2012	Daniel Danzberger