strongSwan - Feature #366

unity plugin can't handle single SPLIT_INCLUDE attribute containing several subnets

25.07.2013 23:07 - Gerald Turner

Status:	Closed	**Start date:**	25.07.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.1.0		
Resolution:	Fixed		

Description

Hi, I'm connecting to a poorly configured Cisco ASA5550 Version 8.4(4)1 that's out of my control. It sends a single SPLIT_INCLUDE attribute containing 54 subnets. charon outputs "handling UNITY_SPLIT_INCLUDE attribute failed" and results in a remote traffic selector of 0.0.0.0/0 which is too wide (hijacks local networks).

```
16[ENC] <xo|6> parsing CONFIGURATION_ATTRIBUTE_V1 payload, 764 bytes left
16[ENC] <xo|6> parsing payload from => 764 bytes @ 0x7fe8b4cb19b4
16[ENC] <xo|6>    0: 70 04 02 F4 0A 00 00 00 FF 00 00 00 00 00 00 00  p...............
16[ENC] <xo|6>   16: 00 00 AC 10 00 00 FF F0 00 00 00 00 00 00 00 00  ................
16[ENC] <xo|6>   32: 40 00 00 00 FF FF 00 00 00 00 00 00 00 00 40 1A  @.............@.
16[ENC] <xo|6>   48: 8F 02 FF FF FF FF 00 00 00 00 00 00 40 1D 90 87  ............@...
16[ENC] <xo|6>   64: FF FF FF FF 00 00 00 00 00 00 40 23 00 F0 FF FF  ..........@#....
16[ENC] <xo|6>   80: FF F0 00 00 00 00 00 00 40 23 34 00 FF FF FF 00  ........@#4.....
16[ENC] <xo|6>   96: 00 00 00 00 00 00 40 23 40 00 FF FF E0 00 00 00  ......@#@.......
16[ENC] <xo|6>  112: 00 00 00 00 40 23 72 20 FF FF FF E0 00 00 00 00  ....@#r ........
16[ENC] <xo|6>  128: 00 00 40 32 00 00 FF FF 80 00 00 00 00 00 00 00  ..@2............
16[ENC] <xo|6>  144: 40 44 60 A4 FF FF FF FF 00 00 00 00 00 00 40 DD  @D`...........@.
16[ENC] <xo|6>  160: F5 90 FF FF FF F0 00 00 00 00 00 00 41 6A 02 00  ............Aj..
16[ENC] <xo|6>  176: FF FF FF 00 00 00 00 00 00 00 41 6A 07 08 FF FF  ..........Aj....
16[ENC] <xo|6>  192: FF FF 00 00 00 00 00 00 41 6A 07 09 FF FF FF FF  ........Aj......
16[ENC] <xo|6>  208: 00 00 00 00 00 00 42 59 00 00 FF FF 00 00 00 00  ......BY........
16[ENC] <xo|6>  224: 00 00 00 00 43 58 00 00 FF F8 00 00 00 00 00 00  ....CX..........
16[ENC] <xo|6>  240: 00 00 47 04 00 00 FF FE 00 00 00 00 00 00 00 00  ..G.............
16[ENC] <xo|6>  256: 87 DF 12 63 FF FF FF FF 00 00 00 00 00 00 8B 55  ...c...........U
16[ENC] <xo|6>  272: 34 8D FF FF FF FF 00 00 00 00 00 00 97 75 18 00  4............u..
16[ENC] <xo|6>  288: FF FF FF 00 00 00 00 00 00 00 9B B8 D1 05 FF FF  ................
16[ENC] <xo|6>  304: FF FF 00 00 00 00 00 00 9C 9A 00 00 FF FF FF 00  ................
16[ENC] <xo|6>  320: 00 00 00 00 00 00 9C 9A 02 00 FF FF FF 00 00 00  ................
16[ENC] <xo|6>  336: 00 00 00 00 9C 9A 21 00 FF FF FF 00 00 00 00 00  ......!.........
16[ENC] <xo|6>  352: 00 00 9E 9B 09 0F FF FF FF FF 00 00 00 00 00 00  ................
16[ENC] <xo|6>  368: 9E 9B FE 4A FF FF FF FF 00 00 00 00 00 00 AA 92  ...J............
16[ENC] <xo|6>  384: B1 00 FF FF FF 00 00 00 00 00 00 00 C0 68 AF 00  .............h..
16[ENC] <xo|6>  400: FF FF FF 00 00 00 00 00 00 00 CB 0C DF 63 FF FF  ............c...
16[ENC] <xo|6>  416: FF FF 00 00 00 00 00 00 CD 9E 00 00 FF FF 00 00  ................
16[ENC] <xo|6>  432: 00 00 00 00 00 00 CE 53 40 00 FF FF E0 00 00 00  .......S@.......
16[ENC] <xo|6>  448: 00 00 00 00 CE 6F 00 00 FF FF 00 00 00 00 00 00  .....o..........
16[ENC] <xo|6>  464: 00 00 CE AD 00 00 FF FF 00 00 00 00 00 00 00 00  ................
16[ENC] <xo|6>  480: CF 58 00 00 FF FF 00 00 00 00 00 00 00 00 CF 95  .X..............
16[ENC] <xo|6>  496: AB 00 FF FF FF 00 00 00 00 00 00 00 CF 9B 80 00  ................
16[ENC] <xo|6>  512: FF FF 80 00 00 00 00 00 00 00 D0 6F 8F 8C FF FF  ...........o....
16[ENC] <xo|6>  528: FF FF 00 00 00 00 00 00 D0 8F 00 00 FF FF 00 00  ................
16[ENC] <xo|6>  544: 00 00 00 00 00 00 D0 A3 50 00 FF FF FF 00 00 00  ........P.......
16[ENC] <xo|6>  560: 00 00 00 00 D1 1F 00 00 FF FF 00 00 00 00 00 00  ................
16[ENC] <xo|6>  576: 00 00 D1 A4 18 00 FF FF FF 00 00 00 00 00 00 00  ................
16[ENC] <xo|6>  592: D1 AD 3D 00 FF FF FF 00 00 00 00 00 00 00 D1 DC  ..=.............
16[ENC] <xo|6>  608: 00 00 FF FF 00 00 00 00 00 00 00 00 D8 FA 76 9C  ............v.
16[ENC] <xo|6>  624: FF FF FF FF 00 00 00 00 00 00 D8 16 80 00 FF FF  ................
16[ENC] <xo|6>  640: FF 00 00 00 00 00 00 00 D8 16 9F 00 FF FF FF 00  ................
16[ENC] <xo|6>  656: 00 00 00 00 00 00 D8 32 56 00 FF FF FF 00 00 00  .......2V.......
16[ENC] <xo|6>  672: 00 00 00 00 D8 32 60 00 FF FF E0 00 00 00 00 00  .....2`.........
16[ENC] <xo|6>  688: 00 00 D8 ED 94 00 FF FF FF 00 00 00 00 00 00 00  ................
16[ENC] <xo|6>  704: AC 13 FD 71 FF FF FF FF 00 00 00 00 00 00 AC 13  ...q............
```

```
16[ENC] <xo|6>  720: FD 72 FF FF FF FF 00 00 00 00 00 00 AC 13 FD 74  .r..............t
16[ENC] <xo|6>  736: FF FF FF FF 00 00 00 00 00 00 D1 76 B3 CB FF FF  ...........v....
16[ENC] <xo|6>  752: FF FF 00 00 00 00 00 00 00 00 00 00              ............
16[ENC] <xo|6>   parsing rule 0 ATTRIBUTE_FORMAT
16[ENC] <xo|6>    => 0
16[ENC] <xo|6>   parsing rule 1 ATTRIBUTE_TYPE
16[ENC] <xo|6>    => 28676
16[ENC] <xo|6>   parsing rule 2 ATTRIBUTE_LENGTH_OR_VALUE
16[ENC] <xo|6>    => 756
16[ENC] <xo|6>   parsing rule 3 ATTRIBUTE_VALUE
16[ENC] <xo|6>    => 756 bytes @ 0x7fe8b4cb6a40
16[ENC] <xo|6>    0: 0A 00 00 00 FF 00 00 00 00 00 00 00 00 00 AC 10  ................
```

I've re-built strongSwan with the patches from bug #356 which helps quite a bit - I can manually specify rightsubnet, ignoring what the Cisco ASA is trying to send. The patch to the create_ts function that allows > 8 bytes isn't effective - I still get "handling UNITY_SPLIT_INCLUDE attribute failed" (I was expecting it to parse the first subnet only, oh well). OTOH the patch to the narrow_initiator function that fallsback on rightsubnet if no UNITY_SPLIT_INCLUDE were handled is working great.

Could unity get updated to handle multipe subnets in a single attribute?

strongswan.conf:

```
charon {
  cisco_unity = yes
  i_dont_care_about_security_and_use_aggressive_mode_psk = yes

  syslog {
    daemon {
      default = 3
      ike_name = yes
    }
  }
}
```

ipsec.conf:

```
conn xo
  auto = add
  aggressive = yes
  authby = xauthpsk
  dpdaction = restart
  keyexchange = ikev1
  esp = aes128-sha1-modp1024
  ike = 3des-md5-modp1024
  left = %any
  leftid = @vpnstandard3
  leftsourceip = %config4
  right = 205.158.160.204
  rightsubnet = 10.0.0.0/8
  xauth_identity = gturner
```

Associated revisions

Revision 1cf80228 - 29.07.2013 21:44 - Tobias Brunner

unity: Handle multi-valued UNITY_SPLIT_INCLUDE/UNITY_LOCAL_LAN attributes

Cisco devices seem to add 6 bytes of padding between each address/mask
pair.

Fixes #366.

History

#1 - 26.07.2013 09:06 - Tobias Brunner

- Tracker changed from Issue to Feature

- Category changed from libstrongswan to libcharon

- Status changed from New to Assigned

- Assignee set to Tobias Brunner

#2 - 26.07.2013 09:52 - Tobias Brunner

- File 0001-unity-Handle-multi-valued-UNITY_SPLIT_INCLUDE-UNITY_.patch added

- Status changed from Assigned to Feedback

> The patch to the create_ts function that allows > 8 bytes isn't effective - I still get "handling UNITY_SPLIT_INCLUDE attribute failed" (I was expecting it to parse the first subnet only, oh well).

That seems odd. Are you sure the patch is applied (and that you actually use the patched version)?

Anyway, the attached patch tries to add support for multi-valued unity attributes. It would be great if you could try it.

#3 - 26.07.2013 23:55 - Gerald Turner

Yep it was odd that the >8bytes patch from bug #356 didn't work.

Neither did this patch :(

I sprinkled the source with some braindead DBG statements and isolated the problem:

The traffic_selector_create_from_bytes function (libstrongswan/selectors/traffic_selector.c) is returning NULL because to.len > 4.

I kludged this function to accpet to.len > 4 (and hardcode the memcpy to only copy 4 bytes), and it works - no more "handling UNITY_SPLIT_INCLUDE attribute failed".

```
          xo[3]: ESTABLISHED 17 seconds ago, 10.88.22.162[vpnstandard3]...205.158.160.204[205.158.160.204]
          xo[3]: IKEv1 SPIs: a8063a9ca8ac6e08_i* cc37fdb40d81e024_r, pre-shared key+XAuth reauthentication in
2 hours
          xo[3]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
          xo{3}:  INSTALLED, TUNNEL, ESP in UDP SPIs: ce974807_i 0c3616cd_o
          xo{3}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 45 minutes
          xo{3}:   172.31.101.25/32 === 10.0.0.0/8 172.16.0.0/12 64.0.0.0/16 64.26.143.2/32 64.29.144.135/32
                   64.35.0.240/28 64.35.52.0/24 64.35.64.0/19 64.35.114.32/27 64.50.0.0/17 64.68.96.164/32
                   64.221.245.144/28 65.106.2.0/24 65.106.7.8/32 65.106.7.9/32 66.89.0.0/16 67.88.0.0/13
                   71.4.0.0/15 135.223.18.99/32 139.85.52.141/32 151.117.24.0/24 155.184.209.5/32 156.154.0.0/
24
                   156.154.2.0/24 156.154.33.0/24 158.155.9.15/32 158.155.254.74/32 170.146.177.0/24 192.104.1
75.0/24
                   203.12.223.99/32 205.158.0.0/16 206.83.64.0/19 206.111.0.0/16 206.173.0.0/16 207.88.0.0/16
                   207.149.171.0/24 207.155.128.0/17 208.111.143.140/32 208.143.0.0/16 208.163.80.0/24 209.31.
0.0/16
                   209.164.24.0/24 209.173.61.0/24 209.220.0.0/16 216.250.118.156/32 216.22.128.0/24 216.22.15
9.0/24
                   216.50.86.0/24 216.50.96.0/19 216.237.148.0/24 172.19.253.113/32 172.19.253.114/32 172.19.2
53.116/32
                   209.118.179.203/32
```

Awesome!

I am a little confused about having to set *rightsubnet=0.0.0.0/0* in order to get the responders split-include selectors. If I remove rightsubnet from the configuration I get an SA failure with message *"no acceptable traffic selectors found"*. This is kind of interesting, I can be more selective about which subnets I actually want (instead of all 54!), and I can also make a mistake and add a non-exsistent subnet to rightsubnets and the process of narrowing traffic selectors eliminates it, cool.

#4 - 27.07.2013 09:18 - Tobias Brunner

- File 0001-unity-Handle-multi-valued-UNITY_SPLIT_INCLUDE-UNITY_.patch added

> The traffic_selector_create_from_bytes function (libstrongswan/selectors/traffic_selector.c) is returning NULL because to.len > 4.

Ah, yes. It's kind of obvious, once pointed out. I updated the patch so that the mask/to address has the proper length.

#5 - 29.07.2013 19:30 - Gerald Turner

Tested the patch, it works great, thanks Tobias!

#6 - 29.07.2013 21:46 - Tobias Brunner

- Status changed from Feedback to Closed

- Target version set to 5.1.0

- Resolution set to Fixed

Thanks for testing the patch. I applied it to master for inclusion in 5.1.0.

Files

charon.log	280 KB	25.07.2013	Gerald Turner
0001-unity-Handle-multi-valued-UNITY_SPLIT_INCLUDE-UNITY_.patch	6.81 KB	26.07.2013	Tobias Brunner
0001-unity-Handle-multi-valued-UNITY_SPLIT_INCLUDE-UNITY_.patch	6.91 KB	27.07.2013	Tobias Brunner