strongSwan - Bug #3627

swanctl - segmentation fault during loading encrypted private key

10.11.2020 17:12 - Jiri Zendulka

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.9.2		
Affected version:	5.8.4	**Resolution:**	Fixed

Description

There is "segmentation fault" error during swanctl --load-all (--load-credential) if encrypted private key is used. If private key is not encrypted then it works.

```
#  /usr/libexec/ipsec/swanctl --load-all
loaded certificate from '/etc/swanctl/x509/local-cert4.pem'
loaded certificate from '/etc/swanctl/x509/remote-cert4.pem'
loaded certificate from '/etc/swanctl/x509ca/cacert4.pem'
Segmentation fault

private-4 {
  file = local-privkey4.pem
  secret = conel000
}

# cat /etc/swanctl/private/local-privkey4.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,5015B67B3FB2D3F9
Zt28RJhFOUKUvYDCANRwRdztvPp7ZbVWcQNSjQf8vabQfQgjEGmzrxnepK4u2MuY
mdCCsTC4kElt5OUeyCFqQsHDHjTw3H3ZDacx63+LvUOWEV9vwJM2pqUo2v0B2eKM
+3rVEs6Ug1CP4Hl6OTvyy3chuYTH+Qsxom5nHsPdU58QrO7e36GXlLhNvfgLDtQA
hE4Drz0zQqPgCMoOLoibVH+fs8DQRTXjKg3XfRxSJG00OeyRjqNm5iQrImumGyLi
3yX3EyqYDORqKGTfi3vKbI4dS3mmMjuHuh5YBQ9hgCxZ79jisRdcVG9hwVY2xlhE
0R25a5jclZhYkG0huUulNGJkH7uRb7/37vfVpMUFCSaa4yYoZjQdvsV4NcTFhyjv
Dm0D50FPPY6Zun7QAtMtmEA/depQsvm2HDRwiig+ebd/gOFwI69GLlNZc68jHUo+
rp143a2vfJ/TORrVonFBi677zsYEmg0V4NSgQ0GozHTY32Hq78oaTKCE90Cmijpm
SQmC4fXHh4RCqI0BGnFvkazTEuXlmwPu///5p+20F44o8Ry2ZU5J2IinGfxDZokb
Aj9dLRGHQ5xfrSrZI0XZHj39694Wbv/sib30J6mCILqohBxPORXqWLJ7yE6bwW0S
vvcf5587YGJYYP9NBeFbS+8+YQh3yQivONS8wqUWSG31lXgrl7SNgNKb2TkLaB5C
fUxkszSo3UcEKShQe8kq9Z6QMpi3wgFNztwnqXOREB1k2LBhK5PhPoF/frOlAmaR
9y9FUETcu3+6WF3jGqvKIZX/AYfBYC3E+OqvFfTvQUsk4SmavHLtN14sHnriGyqP
KYcpaNqvZ+0mG6dbJMKMBTJgwNyluPixOazLUG5nFdaHVqdpL2agKSgE0wcDLUHo
aTI0Y92DlHrCdDbdyLNoYhDUuRD5KaJA7oC2xUIFU7+A5pwPsbDWFxTDLdY/oWcy
xD5ZAzKBQcU8ixhbgXoqlVwotLsWfdP1q7XP+czNqgw/EgqDLyzwRnVtXG12eXc7
bqaHAE1oTpTGlfojShgopBivACaqVCWaFpjEQQaAbculP6WqwruMXaMS1YnwkAcP
Z/tDFMarGcchNOQmRbOz1jWP3gro8+3JIujavMQ9R3RAkDCwnNy77RZzcJObn/sm
Nx8rQcxVPB5S284V69YzlbYIJVZWKp9Zi0vo4phVYKkwdTQoOZ4CN8oDb+oBthfd
41AJRsMmUCE8To1Q2OfLeZlNqBfGYLAldLilJFB4hB8euSwniQZX/TMJXjKIdg3o
+O01Q95iQbwj6eyGF8ftAEPRijcRy13YLcYE96YZYd6B+3H23HM1eAD5uH5ZiLzY
BhXRTn677KPQBVzpjS9ybPM592i9oyc659BSAp5ImK7DMBX9A/vJ5orx1773nHdI
HOCB+WB3r5rJpD5z3ag99D1pPJ2H4KS7vt7DnSgElvqQlh6rKBY7Lst9fxgCSdPJ
LC8Osw0egeDrwDe0peEqFtdyU0vwIgCrqmwl3e2U2qgprAfUgl/XViBxEG/uW5tR
sabkyWyBGTBmXmL/LZIwjk0RstaHrib2vbaCDCXCswmXo2xaCfyTWKxqO25ZicIr
-----END RSA PRIVATE KEY-----
```

Associated revisions

Revision abb3f67b - 13.11.2020 16:40 - Tobias Brunner

pem: Make sure we actually parsed some data

This could happen if there is no separating empty line between header

and body.

References #3627.

History

#1 - 10.11.2020 18:20 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to libstrongswan

- Status changed from New to Feedback

- Target version set to 5.9.2

The file is not correctly formatted. There must be an empty line between header and Base64-encoded body of the PEM file, that is, it should be:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,5015B67B3FB2D3F9

Zt28RJhFOUKUvYDCANRwRdztvPp7ZbVWcQNSjQf8vabQfQgjEGmzrxnepK4u2MuY
...
```

What tool generated this?

Anyway, it should obviously not crash with such a file. I pushed a fix for that to the *3627-pem-fix* branch.

#2 - 11.11.2020 09:55 - Jiri Zendulka

I see. The empty line was removed during importing encrypted key to our device. So there is a bug on our side too.
You can close the issue.

Many thanks.

#3 - 13.11.2020 16:41 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed