

## strongSwan - Bug #1362

### pki --issue segfaults when printing usage output

20.03.2016 23:05 - Noel Kuntze

<b>Status:</b>	Closed	<b>Start date:</b>	20.03.2016
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Tobias Brunner	<b>Estimated time:</b>	0.00 hour
<b>Category:</b>	pki		
<b>Target version:</b>	5.4.0		
<b>Affected version:</b>	5.3.5	<b>Resolution:</b>	Fixed

#### Description

Hello,

ipsec pki reproducibly segfaults with glibc version 2.23 in the strlen function.

glibc version is 2.23

openssl version is 1.0.2.g

Command run: pki --issue --in style.key -t rsa --out style.pem --digest sha256 --dn "C=DE, O=ThermiCorp, CN=Thermis Style" --cacert userca.pem --cakey private/userca.key --inform der --outform pem

#### Stack trace:

```
Mär 20 22:58:43 thermi-pc.thermicorp.lan systemd-coredump[13413]: Process 13411 (pki) of user 1000 dumped core.
```

Stack trace of thread 13411:

```
#0 0x00007f442f949646 strlen (libc.so.6)
#1 0x00007f442f911c7 printf_positional (libc.so.6)
#2 0x00007f442f911c76 vfprintf (libc.so.6)
#3 0x00007f442f914691 buffered_vfprintf (libc.so.6)
#4 0x00007f442f911afd vfprintf (libc.so.6)
#5 0x00007f442f9c0c39 __fprintf_chk (libc.so.6)
#6 0x0000000000404490 fprintf (pki)
#7 0x0000000000405719 issue (pki)
#8 0x00007f442f8eb710 __libc_start_main (libc.so.6)
#9 0x0000000000403af9 _start (pki)
```

#### gdb debugging yields this:

```
#0 0x00007ffff7857646 in strlen () from /usr/lib/libc.so.6
No symbol table info available.
#1 0x00007ffff781f1c7 in printf_positional () from /usr/lib/libc.so.6
No symbol table info available.
#2 0x00007ffff781fc76 in vfprintf () from /usr/lib/libc.so.6
No symbol table info available.
#3 0x00007ffff7822691 in buffered_vfprintf () from /usr/lib/libc.so.6
No symbol table info available.
#4 0x00007ffff781fafd in vfprintf () from /usr/lib/libc.so.6
No symbol table info available.
#5 0x00007ffff78cec39 in __fprintf_chk () from /usr/lib/libc.so.6
No symbol table info available.
#6 0x0000000000404490 in fprintf (__fmt=0x40b8aa ' ' <repeats 14 times>, "%s\n", __stream=0x7ffff7b75520 <_IO_2_1_stderr_>) at /usr/include/bits/stdio2.h:97
No locals.
#7 command_usage (error=error@entry=0x40be20 "invalid output format") at command.c:220
    out = 0x7ffff7b75520 <_IO_2_1_stderr_>
    i = 11
#8 0x0000000000405719 in issue () at commands/issue.c:572
    form = CERT_ASN1_DER
    digest = <optimized out>
    cert_req = 0x0
```

```
cert = 0x0
ca = 0x0
private = 0x0
public = 0x0
type = CRED_PRIVATE_KEY
subtype = KEY_RSA
pkcs10 = false
file = 0x7fffffff3bc "style.key"
dn = 0x0
hex = 0x0
cacert = 0x0
cakey = 0x0
error = 0x40be20 "invalid output format"
keyid = 0x0
id = 0x0
san = 0x637450
cdps = 0x637510
ocsp = 0x6375d0
permitted = 0x637690
excluded = 0x637750
policies = 0x637810
mappings = 0x6378d0
pathlen = 255
inhibit_any = 255
inhibit_mapping = 255
require_explicit = 255
serial = {ptr = 0x0, len = 0}
encoding = {ptr = 0x0, len = 0}
not_before = 0
not_after = 0
lifetime = <optimized out>
datenb = 0x0
datena = 0x0
dateform = 0x0
flags = X509_NONE
x509 = <optimized out>
cdp = <optimized out>
policy = 0x0
arg = 0x7fffffff3d3 "style.pem"
#9 0x00007ffff7f9710 in __libc_start_main () from /usr/lib/libc.so.6
No symbol table info available.
#10 0x000000000403af9 in _start ()
No symbol table info available.
```

## History

### #1 - 21.03.2016 11:10 - Tobias Brunner

- Tracker changed from Issue to Bug
- Subject changed from pki segfault in libc to pki --issue segfaults when printing usage output
- Category set to pki
- Status changed from New to Closed
- Assignee set to Tobias Brunner
- Target version set to 5.4.0
- Resolution set to Fixed

This has already been fixed with [8ea64a78d6](#) and [50e190e8ad](#), was originally [reported at github.com](#).

By the way, the reason for the "invalid output format" error is that --out style.pem triggers the argument handler for the --outform|-f option, there is no --out option.