strongSwan - Bug #633

esp=cast128 broken

04.07.2014 08:23 - Paul Wouters

Status:	Closed	**Start date:**	04.07.2014
Priority:	Low	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	libhydra		
Target version:	5.2.0		
Affected version:	5.1.3	**Resolution:**	Fixed

Description

While performing interop testing, I noticed a bug in ESP_CAST handling
in strongswan:

Jul 4 02:05:57 13[KNL] using encryption algorithm CAST_CBC with key size 128
Jul 4 02:05:57 13[KNL] using integrity algorithm HMAC_SHA1_96 with key size 160
Jul 4 02:05:57 13[KNL] using replay window of 32 packets
Jul 4 02:05:57 13[KNL] sending XFRM_MSG_NEWSA: => 420 bytes @ 0x7ffddacb9610
[...]
Jul 4 02:05:57 13[KNL] received netlink error: Function not implemented (38)
Jul 4 02:05:57 13[KNL] unable to add SAD entry with SPI 8d5e4bbc

The netlink code is using the wrong name for cast. It is possible this
been changed in the Linux kernel at some point (possibly when cast6 was
added). The following patch should fix it - untested but the code is
similar to libreswan:

```
diff --git a/src/libhydra/plugins/kernel_netlink/kernel_netlink_ipsec.c b/src/libhydra/plugins/kernel_netlink/kernel_netlink_ipsec.c
index 55c2f34..549ed2f 100644
--- a/src/libhydra/plugins/kernel_netlink/kernel_netlink_ipsec.c
+++ b/src/libhydra/plugins/kernel_netlink/kernel_netlink_ipsec.c
@ -177,7 +177,7 @ static kernel_algorithm_t encryption_algs[] = {        {ENCR_3DES,                    "des3_ede"
},
/*    {ENCR_RC5,                    "***"                    }, /
/    {ENCR_IDEA,                    "***"                    }, */
-      {ENCR_CAST,                    "cast128"                },
+      {ENCR_CAST,                    "cast5"                },        {ENCR_BLOWFISH,                    "blowfish"                },
/*    {ENCR_3IDEA,                "***"                    }, /
/    {ENCR_DES_IV32,                "***"                    }, */
```

Associated revisions

Revision 83995109 - 04.07.2014 10:18 - Martin Willi

kernel-netlink: Rename algorithm identifier from cast128 to cast5

Even if the XFRM identifier was named cast128 in the kernel before 2.6.31, it
actually never worked, because there is no such crypto algorithm.

The identifier has been changed to cast5 in
https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=245acb87
to make it work, so we should use that.

Fixes #633.

History

#1 - 04.07.2014 09:20 - Martin Willi

- Status changed from New to Assigned

- Assignee set to Martin Willi

#2 - 04.07.2014 10:01 - Martin Willi

Paul,

Thanks for your bug report.

> The netlink code is using the wrong name for cast. It is possible this been changed in the Linux kernel at some point

In fact has this identifier been changed for 2.6.31. Have to test it if that ever worked with the old identifier and if we need a fallback solution.

Regards
Martin

#3 - 04.07.2014 10:23 - Martin Willi

- Status changed from Assigned to Closed

- Resolution set to Fixed

CAST never worked with that identifier, and Herbert is right that *nobody has ever used it* :)

So we can avoid any compatibility option, and just rename the identifier. I've applied the fix with the referenced commit.

Regards
Martin

#4 - 04.07.2014 10:52 - Martin Willi

- Tracker changed from Issue to Bug

- Target version set to 5.2.0