strongSwan - Bug #3064

curve448 does not appear to be recognized as valid in ike or esp config

17.05.2019 17:01 - Jim Pingle

Status:	Closed	**Start date:**	17.05.2019
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.8.0		
Affected version:	dr|rc|master	**Resolution:**	Fixed

Description

On FreeBSD 12 with strongSwan 5.8.0.d2, I can use curve25519 with IKEv1 and IKEv2 when the curve25519 plugin is loaded, but curve448 does not work with either IKEv1 or IKEv2.

In ipsec.conf, I specified it like this:

```
    ike = aes256-sha1-curve448!
    esp = aes256-sha256-curve448!
```

That syntax works if I use curve25519 instead, but when attempting to use curve448, strongSwan acts as though no DH was selected:

```
configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ
```

I also don't see curve448 listed in https://github.com/strongswan/strongswan/blob/master/src/libstrongswan/crypto/proposal/proposal_keywords_static.txt along with the others, though it is listed on https://wiki.strongswan.org/projects/strongswan/wiki/IKEv2CipherSuites which says it should be a valid keyword for ike or esp.

It's also missing from https://wiki.strongswan.org/projects/strongswan/wiki/IKEv1CipherSuites but that may be intentional, though curve25519 is listed there as well.

Related issues:

Related to Issue #3065: Error building 5.8.0rc1 without gperf	**Closed**

Associated revisions

Revision fbfe5a27 - 20.05.2019 09:43 - Tobias Brunner

proposal: Add missing curve448/x448 keywords

Fixes #3064.

History

#1 - 17.05.2019 17:19 - Tobias Brunner

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Target version set to 5.8.1

- Resolution set to Fixed

Thanks for the report. Fix is in the *3064-curve448-keyword* branch.

> It's also missing from https://wiki.strongswan.org/projects/strongswan/wiki/IKEv1CipherSuites but that may be intentional, though curve25519 is listed there as well.

Yeah, didn't update that page in a while (using either of these algorithms with IKEv1 is not standardized anyway).

#2 - 17.05.2019 18:05 - Tobias Brunner

- Related to Issue #3065: Error building 5.8.0rc1 without gperf added

#3 - 17.05.2019 22:07 - Jim Pingle

It works as expected with the change from that branch, thanks!

Log entries:

```
charon[31462]: 15[CFG] <2> received proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/CURVE_448
charon[31462]: 15[CFG] <2> configured proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/CURVE_448
charon[31462]: 15[CFG] <2> selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/CURVE_448
```

ipsec statusall output:

```
con5000[2]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/CURVE_448
```

#4 - 20.05.2019 09:51 - Tobias Brunner

- Status changed from Feedback to Closed

- Target version changed from 5.8.1 to 5.8.0