strongSwan - Bug #172

Support X509 certificates without CA basic constraints

28.01.2012 04:50 - Nikolay bryskin

Status:	Closed	**Start date:**	28.01.2012
Priority:	Low	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	4.6.2		
Affected version:	4.6.1	**Resolution:**	

Description

charon fails to load X509 CA certificates without CA basic constraints. Here is patch that adds this functionality.

History

#1 - 30.01.2012 13:23 - Tobias Brunner

- Status changed from New to Feedback

- Priority changed from Normal to Low

The problem with this is that it enables any user with a valid client certificate to issue arbitrary certificates, hence, allowing them to perform man-in-the-middle attacks.
Therefore, this patch won't make it into any strongSwan release.

#2 - 31.01.2012 18:48 - Nikolay bryskin

I agree that my patch is too permissive, but I'm using it because of http://www.tbs-x509.com/GTECyberTrustGlobalRoot2018.crt that is version 1 X509 and hasn't any extensions, including basic constraints. My be we should check for certificate version before checking CA constraints?

#3 - 01.02.2012 13:28 - Tobias Brunner

- File ignore_missing_ca_basic_constraint.patch added

- Category set to charon

- Assignee set to Tobias Brunner

I see. It seems there are a few older CA root certificates without basic constraint still in use (on my Ubuntu system I got over 20 of them).

Would the attached patch work for you? It allows to force the stroke plugin (charon.plugins.stroke.ignore_missing_ca_basic_constraint in strongswan.conf) to treat certificates in /etc/ipsec.d/cacert and listed in ipsec.conf ca sections as CA certificates even if they lack a CA basic constraint.

#4 - 01.02.2012 13:47 - Martin Willi

Looks fine to me.

I think we could even avoid set_flags() by passing the flag to the builder (BUILD_X509_FLAG).

#5 - 01.02.2012 14:39 - Tobias Brunner

- Target version set to 4.6.2

> I think we could even avoid set_flags() by passing the flag to the builder (BUILD_X509_FLAG).

Yep. Changed the patch and committed it to master (see 9ec66bc).

#6 - 06.02.2012 10:47 - Tobias Brunner

- Status changed from Feedback to Closed

Files

charon-cert-without-ca-basic-constraints.patch	4.16 KB	28.01.2012	Nikolay bryskin
ignore_missing_ca_basic_constraint.patch	5.23 KB	01.02.2012	Tobias Brunner