AqBanking - Bug #295

Falsche Meldung "Zertifikat-Besitzer passt nicht zum Hostnamen"

16.04.2023 14:18 - mlenk

Status:	Resolved	**Beginn:**	16.04.2023
Priorität:	High	**Abgabedatum:**	
Kategorie:	Gwenhywfar		
Betriebssystem:	Linux	**Anwendung:**	aqbanking-cli
AqBanking-Version:	6.2.10	**Version der Anwendung:**	

Beschreibung

Hallo Martin,

Seit ein paar Tagen funktioniert die Kommunikation mit den Servern z.B. der GLS Bank nicht mehr. Es kommt die Meldung "Zertifikat-Besitzer passt nicht zum Hostnamen". Konfiguriert ist schon sehr lange die URL https://hbci-pintan.gad.de/cgi-bin/hbciservlet, d.h. es wird erwartet, dass das Zertifikat für den Hostnamen hbci-pintan.gad.de gültig ist.

Schaut man sich das vom Server vorgelegte Zertifikat näher an, ist leider festzustellen, dass dieses tatsächlich (auch) für hbci-pintan.gad.de gültig ist. In der Zertifikatserweiterung SubjectAltName (SAN) wird hbci-pintan.gad.de korrekt aufgeführt.

Zitat von https://en.wikipedia.org/wiki/Subject_Alternative_Name

> RFC 2818 (May 2000) specifies Subject Alternative Names as the preferred method of adding DNS names to certificates, deprecating the previous method of putting DNS names in the commonName field.[3] Google Chrome version 58 (March 2017) removed support for checking the commonName field at all, instead only looking at the SANs.

Wenn das Zertifikat also gültig ist aber von AqBanking nicht als korrekt akzeptiert wird, liegt hier wohl ein Bug vor.

Ich habe mich gleich im Code auf die Suche gemacht. Anscheinend ist die inkorrekte Prüfung in src/sio/syncio_tls.c an dieser Stelle:

```
      rv=gnutls_x509_crt_get_dn_by_oid(cert, GNUTLS_OID_X520_COMMON_NAME, 0, 0, buffer1, &size);
      if (rv==0) {
        GWEN_SslCertDescr_SetCommonName(certDescr, buffer1);
        if (xio->hostName && strcasecmp(xio->hostName, buffer1)!=0) {
          DBG_INFO(GWEN_LOGDOMAIN, "Owner of certificate does not match hostname");
          errFlags|=GWEN_SSL_CERT_FLAGS_BAD_HOSTNAME;
        }
```

Hier wird offenbar nur der Common Name aus dem Zertifikat geprüft, aber nicht die "Subject Alt Name"-Erweiterung.

Gibt es einen Grund, warum in Gwenhywfar die Prüfung von Hand implementiert hat, obwohl GnuTLS die Verifikation des Hostnames (und vieler anderer Parameter) schon von Haus aus macht (API-Funktion gnutls_session_set_verify_cert)?

Historie

#1 - 16.04.2023 14:32 - mlenk

Sieht so aus als sei die Hostname-Validierung des Zertifikats doppelt implementiert (gleiche Datei):

```
        DBG_INFO(GWEN_LOGDOMAIN, "Checking hostname [%s]", xio->hostName);
        if (!gnutls_x509_crt_check_hostname(cert, xio->hostName)) {
          DBG_WARN(GWEN_LOGDOMAIN,
                   "Certificate was not issued for this host");
          GWEN_Gui_ProgressLog(0, GWEN_LoggerLevel_Warning,
                               I18N("Certificate was not issued for this host"));
          errFlags|=GWEN_SSL_CERT_FLAGS_BAD_HOSTNAME;
        }
```

Diese Implementierung sieht vollkommen ausreichend aus.

#2 - 16.04.2023 15:00 - mlenk

Wenn man die Zeilen 1044 bis 1047 löscht, ist das Problem behoben.
Ein nicht zum Hostnamen passendes Zertifikat wird dann trotzdem korrekterweise als potentielles Problem angezeigt.

Ich lösche diese Zeilen mal im Git.

#3 - 16.04.2023 15:20 - mlenk

- Status wurde von New zu Resolved geändert

Fix committed:
https://www.aquamaniac.de/rdm/projects/gwenhywfar/repository/revisions/a901426cfa0d555b7920dc39358af293dedafe85

#4 - 18.04.2023 23:00 - mlenk

Nur der Vollständigkeit halber, ich habe diesen Bug auch im Debian-Bugtracker erfasst
https://bugs.debian.org/1034577