AqBanking - Bug #41

Signieren RDH-10 (sha256 / sha256sha256)

09/09/2019 06:24 PM - thbe

Status:	New	**Start date:**	09/09/2019
Priority:	Normal	**Due date:**	
Category:	AqBanking		
Betriebssystem:		**Anwendung:**	
AqBanking-Version:		**Version der Anwendung:**	

Description

Hallo.

https://lists.aquamaniac.de/private/aqbanking-user/2019-September/005533.html

Arrgh.
Irgendwas stimmt hier nicht ^^

In 5.7.8 wird ein- bzw. zweimal gehasht. In 5.99.xx kein- bzw. einmal.
(msgcrypt_rdh10.c 297 / msgcrypt_rxh_common.c ab 688)

Nun könnte der Fix sein, das in 5.99.xx auch wieder so zu machen.
Aber: warum funktioniert dann z.B. RDH-7 (laut einiger Nutzer)?
Meine Vermutung ist, dass - warum auch immer - der (ein) Hash auf der Karte stattfindet, da find ich aber nichts wo das sein soll.
(Überhaupt finde ich nur einen Aufruf von GWEN_Crypt_Token_SetSignFn, den in ctfile.c)
Sollte es so sein könnte der Fix drin bestehen, das nur bei Datei-token in msgcrypt_rxh_common.c ein bzw. zweimal zu hashen.

Irgendwelche Meinungen?

Ah und verify, hier wird unterschiedlich vorgegangen, also Segmentkopf und -daten getrennt gehasht,
das ist korrekt?

Gruss,
Thomas

History

#1 - 09/09/2019 11:30 PM - thbe

- File aqbanking-sign.patch added

Ein patch dafür, q&d, hoffentlich nicht zu sehr (Ist auch nicht mehr soo früh am Tag jetzt) anbei.

(siehe auch https://lists.aquamaniac.de/private/aqbanking-user/2019-September/005540.html)

Berücksichtigt momentan nur RDH|RAH-10.
Zu klären wäre u.a. noch, warum das nur (?) bei Schlüsseldatei nötig ist.

Was mir grade aufgefallen ist beim testen, habe dazu 'aqhbci-tool4 getsysid' genommen, ist:

Fehlerhafte Nachrichten-Nummer (ignoriert)

Das kommt wohl, weil zwei mal HKEND verschickt wird.

Das, bzw. das zwangsweise Beenden eines Dialogs seit 55.99.25 ist aber ein anderes, möglicherweise
interessant werdendes Thema.

Gruss,
Thomas

#2 - 09/10/2019 08:37 AM - thbe

- File aqbanking-sign-2.patch added

Was mich ja etwas störte war, dass ich GWEN_Crypt_Token_SetSignFn nur einmal in ctfile.c fand.
Hätte ich da gesucht, wo es noch vorkommt - in libchipcard - wäre mir eher einiges klarer ^^
Also der zweite Hash passiert auf der Karte (DF_SIG).
Daher jetzt der patch so, dass nach dem tokentype geschaut wird und wenn ohbci, der (2.) Hash durchgeführt wird.
Einfaches sha256 wird nicht berücksichtigt, so weit ich das überblicke kommt das nur bei Karte vor.

#3 - 09/11/2019 12:47 AM - martin

Moin Thomas,

Patch ist im GIT, vielen Dank.

Das mit dem doppelten HKEND sollte inzwischen auch wieder gefixed sein. Hatte mit dem Umbau fuer SCA zu tun...

Gruss
Martin

#4 - 09/11/2019 09:14 AM - thbe

- File aqbanking-sign-rxh-kv.patch added

Moin Martin,

jo sehr schön, es wurde ja auch schon erfolgreich an einer echten Bank getestet:
https://lists.aquamaniac.de/private/aqbanking-user/2019-September/005563.html

Ich habe eben noch etwas entdeckt, beim Signieren wird die keyversion fest auf '1' gesetzt:

rv=AH_MsgRxh_PrepareCryptoSeg(hmsg, su, rxh_parameter, rxh_parameter->protocolVersion, 1, ki, cfg, 0, 1);

Das klappt dann nicht mehr, wenn man seine Schlüssel erneuert hat (was aber bisher ja eh nicht geht).

Patch dafür tu ich mal mit hier rein.

Das zwangsweise HKEND jetzt ist aber evtl. noch ein Problem, da es zumindest einen Fall gibt, wo der Server
mitteilt keines mehr haben zu wollen. Nach einem Schlüsselwechsel **kann** ein '3250 Schlüssel wurden gesperrt. Endenachricht nicht mehr möglich.' folgen.

Gruss,
Thomas

#5 - 10/03/2019 02:14 PM - martin

- Category set to AqBanking

Files

aqbanking-sign.patch	2.13 KB	09/09/2019	thbe
aqbanking-sign-2.patch	1.96 KB	09/10/2019	thbe
aqbanking-sign-rxh-kv.patch	795 Bytes	09/11/2019	thbe