reverse proxy - Bug #39

Disable old cipher suites and strenghten forward secrecy

07/13/2020 09:48 PM - Martin Rpunkt

Status:	Closed	**Start date:**	07/13/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

Siehe https://www.ssllabs.com/ssltest/analyze.html?d=zom.bi&hideResults=on
zom.bi unterstützt viele alte, nicht mehr sichere Cipher-Suites, das Problem kann mit folgender config in der traefik.toml umgangen werden:

[tls.options]
[tls.options.default]
minVersion = "VersionTLS12"
#sniStrict = true #Anschalten, falls möglich
cipherSuites = [
"TLS_CHACHA20_POLY1305_SHA256",
"TLS_AES_128_GCM_SHA256",
"TLS_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
]
[tls.options.mintls13]
minVersion = "VersionTLS13"

Entsprechender Code wurde bereits außerhalb der zom.bi infrastruktur getestet und für funktionsfähig befunden.

History

#1 - 11/05/2020 09:36 AM - Chris -

Da ich in letzter Zeit bei meinen Kollegen auch bisschen Werbung für das Setup gemacht habe und die das tatsächlich auch nutzen, ist das einem von denen das Problem auch aufgefallen (Danke Tom ;)).

Ich denk' mal, ich werd mir das kommende Wochenende mal anschauen, wie ich das Konfig-Snippet in den Container bekomme.

#2 - 11/05/2020 07:43 PM - Chris -

hab die Konfiguration im .toml File angepasst.
https://git.zom.bi/zombi/proxy/pulls/1

#3 - 11/05/2020 07:43 PM - Chris -

- Status changed from New to In Progress

#4 - 11/05/2020 09:51 PM - Chris -

Angepasste Konfig ist hinterlegt, wird aber scheinbar nicht aktiv. Gibt keinen Fehler beim Reload oder so aber TLSv1 und TLSv1.1 mit gammel-ciphers sind immer noch aktiv.

#5 - 11/06/2020 05:14 PM - Chris -

habs zum laufen bekommen. Ist scheinbar auch wichtig, wo die Konfiguration liegt:

https://git.zom.bi/zombi/proxy/pulls/2

#6 - 04/09/2021 04:40 PM - Paul S.

- Status changed from In Progress to Closed

Closing this bug, as ssllabs returns A+ rating now: https://www.ssllabs.com/ssltest/analyze.html?d=zom.bi&hideResults=on&latest

(If I read this in the future, on Kubernetes traefik can change endpoint configurations using a TLSOptions CRD.)