

Zéphir - Scénario #27153

EOLE 2.7 devrait supporter TLS 1.1 voire 1.2

03/08/2019 11:40 AM - Thierry Bertrand

Status:	Terminé (Sprint)	Start date:	07/18/2019
Priority:	Normal	Due date:	08/30/2019
Assigned To:	Joël Cuissinat	% Done:	100%
Category:		Estimated time:	0.00 hour
Target version:	sprint 2019 27-35 Equipe MENSUR (été)	Spent time:	0.00 hour
Description			
<p>Actuellement, les négociations TLS sont particulièrement lentes lors de la négociation sur les sites https (1 à 2 secondes). Pour essayer de remédier à cela, j'ai forcé une négociation via TLS 1.1 de la façon suivante :</p> <p>dans firefox, about:config security.tls.version.min changé de 1 à 2 1 => TLS 1.0 2 => TLS 1.1 3 => TLS 1.2</p> <p>Après application, une connexion zephir frontend devient impossible :</p> <p>Échec de la connexion sécurisée</p> <p>Une erreur est survenue pendant une connexion à zephir-04.eole.e2.rie.gouv.fr:8070. Le pair utilise une version non gérée du protocole de sécurité. Code d'erreur : SSL_ERROR_UNSUPPORTED_VERSION</p> <p>La page que vous essayez de consulter ne peut pas être affichée car l'authenticité des données reçues ne peut être vérifiée. Veuillez contacter les propriétaires du site web pour les informer de ce problème.</p> <p>Ce problème semble être provoqué par vos paramètres de sécurité réseau. Voulez-vous restaurer les paramètres par défaut ?</p> <p>Il se peut que TLS 1.1 devienne la version minimum lors des prochaines versions de firefox. Il faudrait ptet l'anticiper.</p>			
Subtasks:			
Tâche # 28770: Passer Zéphir 2.7 en TLS 1.2			Fermé
Tâche # 28772: Passer l'EAD2 en TLS 1.2 sur 2.7			Fermé
Related issues:			
Related to EoleSSO - Scénario #28809: Passer EoleSSO en TLS 1.2 sur EOLE 2.7		Terminé (Sprint)	01/07/2020 01/17/2020

History

#1 - 03/22/2019 02:59 PM - Luc Bourdot

- Tracker changed from Proposition Scénario to Scénario
- Subject changed from zephir devrait supporter TLS 1.1 voire 1.2 to zephir 2.7 devrait supporter TLS 1.1 voire 1.2
- Due date set to 04/12/2019
- Target version set to sprint 2019 13-15 Equipe MENSUR
- Start date set to 03/25/2019

#2 - 03/25/2019 11:32 AM - Joël Cuissinat

- Story points set to 2.0

#3 - 03/25/2019 03:36 PM - Joël Cuissinat

- Assigned To set to Joël Cuissinat

#4 - 05/17/2019 10:11 AM - Joël Cuissinat

- Due date deleted (04/12/2019)
- Assigned To deleted (Joël Cuissinat)
- Target version deleted (sprint 2019 13-15 Equipe MENSJR)
- Start date deleted (03/25/2019)
- Release set to EOLE 2.7.1

#5 - 07/16/2019 03:07 PM - Joël Cuissinat

Piste de travail :

```
>>> from OpenSSL import SSL
>>> print SSL.TLSv1_METHOD, SSL.TLSv1_1_METHOD, SSL.TLSv1_2_METHOD
4 5 6
```

La plupart des outils EOLE utilisent ce paramètre :

- Zéphir : /usr/lib/python2.7/dist-packages/zephir/certificats.py
- EAD : /usr/share/ead2/lib/libsecure.py
- EoleSSO : /usr/lib/python2.7/dist-packages/eolesso/libsecure.py (#FIXME : utilise M2Crypto au lieu de python OpenSSL)

#6 - 07/18/2019 10:15 AM - Joël Cuissinat

- Due date set to 08/30/2019
- Target version set to sprint 2019 27-35 Equipe MENSJR (été)
- Start date set to 07/01/2019

#7 - 07/18/2019 10:15 AM - Joël Cuissinat

- Project changed from conf-zephir to Zéphir

#8 - 07/18/2019 02:20 PM - Joël Cuissinat

- Subject changed from zephir 2.7 devrait supporter TLS 1.1 voire 1.2 to Zéphir 2.7 devrait supporter TLS 1.1 voire 1.2
- Assigned To set to Joël Cuissinat

#9 - 08/20/2019 04:38 PM - Joël Cuissinat

- Related to Scénario #28809: Passer EoleSSO en TLS 1.2 sur EOLE 2.7 added

#10 - 08/20/2019 04:38 PM - Joël Cuissinat

- Subject changed from Zéphir 2.7 devrait supporter TLS 1.1 voire 1.2 to Eole 2.7 devrait supporter TLS 1.1 voire 1.2

#11 - 08/20/2019 04:38 PM - Joël Cuissinat

- Subject changed from *Eole 2.7 devrait supporter TLS 1.1 voire 1.2* to *EOLE 2.7 devrait supporter TLS 1.1 voire 1.2*

#12 - 08/20/2019 04:44 PM - Joël Cuissinat

- Status changed from *Nouveau* to *Terminé (Sprint)*

#13 - 09/04/2019 12:25 PM - Joël Cuissinat

- Release changed from *EOLE 2.7.1* to *EOLE 2.7.1.1*