Lasso - Development #71313

compatibilité xmlsec 1.2.35 (openssl 3?)

15 novembre 2022 10:20 - Frédéric Péters

Statut:	Fermé	**Début:**	15 novembre 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Dans debian est arrivé xmlsec 1.2.36 (c'était 1.2.34 avant);

> October 31 2022
> The XML Security Library 1.2.36 release includes the following changes:
>
> - Retired the XMLSec mailing list "xmlsec@aleksey.com" and the XMLSec Online Signature Verifier.
> - Several other small fixes (more details).
>
> October 25 2022
> The XML Security Library 1.2.35 release includes the following changes:
>
> - Migration to OpenSSL 3.0 API (based on PR by @snargit). Note that OpenSSL engines are disabled by default when XMLSec library is compiled against OpenSSL 3.0. To re-enable OpenSSL engines, use "--enable-openssl3-engines" configure flag (there will be a lot of deprecation warnings).
> - The OpenSSL before 1.1.0 and LibreSSL before 2.7.0 are now deprecated and will be removed in the future versions of XMLSec Library.
> - Refactored all the integer casts to ensure cast-safety. Fixed all warnings and enabled "-Werror" and "-pedantic" flags on CI builds.
> - Added configure flag to use size_t for xmlSecSize (currently disabled by default for backward compatibility).
> - Moved all CI builds to GitHub actions.
> - Several other small fixes (more details).

cette montée de version fait échouer lasso de diverses manières; sur l'initiation d'un SSO,

```
lasso:ERROR:tools.c:586:lasso_query_sign: assertion failed: (rsa)
Bail out! lasso:ERROR:tools.c:586:lasso_query_sign: assertion failed: (rsa)
```

Révisions associées

Révision 66ebd111 - 21 novembre 2022 13:22 - Benjamin Dauvergne

Use OpenSSL EVP API to work around deprecation of low level APIs in OpenSSL 3 (#71313)

OpenSSL API is used to sign query-string values in the SAML 2.0 Redirect binding.
Other binding only need the libxmlsec API as signature are XML DSIG signatures.

Historique

#1 - 15 novembre 2022 12:23 - Benjamin Dauvergne

La source du problème c'est qu'OpenSSL a déprécié les fonctions bas niveaux (RSA_sign, structure RSA) et en mode OpenSSL 3 pure xmlsec ne les expose donc plus, ça casse notre support des signatures avec le binding GET (signature de texte et pas XML) :

```
/**
 * xmlSecOpenSSLKeyDataRsaGetRsa:
 * @data:               the pointer to RSA key data.
 *
 * DEPRECATED. Gets the OpenSSL RSA key from RSA key data.
 *
 * Returns: pointer to OpenSSL RSA key or NULL if an error occurs.
 */
RSA*
```

```
xmlSecOpenSSLKeyDataRsaGetRsa(xmlSecKeyDataPtr data) {
#ifndef XMLSEC_OPENSSL_API_300
    EVP_PKEY* pKey;

    xmlSecAssert2(xmlSecKeyDataCheckId(data, xmlSecOpenSSLKeyDataRsaId), NULL);

    pKey = xmlSecOpenSSLKeyDataRsaGetEvp(data);
    xmlSecAssert2((pKey == NULL) || (EVP_PKEY_base_id(pKey) == EVP_PKEY_RSA), NULL);

    return((pKey != NULL) ? EVP_PKEY_get0_RSA(pKey) : NULL);
#else /* XMLSEC_OPENSSL_API_300 */
    UNREFERENCED_PARAMETER(data);
    xmlSecNotImplementedError("OpenSSL 3.0 does not support direct access to RSA key");
    return(NULL);
#endif /* XMLSEC_OPENSSL_API_300 */
}
```

Je suppose qu'il va falloir reconstruire tout ça au dessus des APIs haut-niveau EVP_* :/

#2 - 15 novembre 2022 17:12 - Benjamin Dauvergne

- Fichier 0001-wip.patch ajouté

- Patch proposed changé de Non à Oui

Avec ça les tests passent mais faut que je redécoupe, beaucoup de trucs sont devenus dépréciés un peu partou.

#3 - 16 novembre 2022 09:31 - Benjamin Dauvergne

Benjamin Dauvergne a écrit :

> Avec ça les tests passent mais faut que je redécoupe, beaucoup de trucs sont devenus dépréciés un peu partout.

Bon ben va falloir gérer xmlsec pre et post 1.2.35 à cause de la dépréciation de xmlSecBase64Decode en plus de la migration vers l'API EVP d'OpenSSL.

#4 - 16 novembre 2022 18:56 - Benjamin Dauvergne

- Fichier 0007-Fix-use-of-wrong-enumeration-NULL-value-71313.patch ajouté

- Fichier 0009-Fix-warning-about-enum-conversion-71313.patch ajouté

- Fichier 0001-Use-OpenSSL-EVP-API-to-work-around-deprecation-of-lo.patch ajouté

- Fichier 0010-Fix-all-cast-function-type-warnings-71313.patch ajouté

- Fichier 0006-Fix-warnings-about-type-casts-71313.patch ajouté

- Fichier 0003-Make-lasso_inflate-output-the-inflated-buffer-size-7.patch ajouté

- Fichier 0008-Fix-all-warnings-in-tests-71313.patch ajouté

- Fichier 0002-Add-new-define-LASSO_XMLSEC_VERSION_NUMBER-allow-ver.patch ajouté

- Fichier 0011-Fix-unused-parameters-warnings-71313.patch ajouté

- Fichier 0005-Replace-all-use-of-xmlSecBase64Decode-by-lasso_base6.patch ajouté

- Fichier 0004-Adapt-lasso_base64_decode-to-the-deprecation-of-xmlS.patch ajouté

- Tracker changé de Bug à Development

- Statut changé de Nouveau à Solution proposée

- 0001: le patch en question
- 0002/0003: réécriture pour prendre en compte que xmlSecBase64Decode est déprécié et que je n'ai aucune idée de quand elle sera définitivement retirée, j'ai mis un #if/#else/#endif pour que ça reste compilable avec libxmlsec<1.2.35
- le reste, des corrections aux warnings il en reste trois sources :
  - g_type_class_add_private qui est déprécié et c'est le gros morceau en attente
  - des trucs autour de distutils dans configure.ac
  - des tas de dépréciations dans autoconf sur sid (je pense que ça peut attendre, c'est juste moche quand on fait autogen.sh)

Ce serait bien que ça passe vite que je puisse faire la release et que le paquet Debian soit correct pour le prochain freeze.

#5 - 16 novembre 2022 20:18 - Frédéric Péters

Pour info déjà,

```
lasso (2.8.0-2) unstable; urgency=medium
.
  * debian/patches/use-openssl-evp-api.diff: import upstream WIP patch for
    compatibility with latest xmlsec (closes: 1024138)
```

Uniquement 0001 donc, et je n'ai pas lu/testé les autres.

Note : dans la branche il y a avant ces commits des commits pas liés ("Release 2.8.1" et "Augment timeout on ECP tests").

#6 - 16 novembre 2022 20:24 - Frédéric Péters

- Sujet changé de compatiblité xmlsec 1.2.35 (openssl 3?) à compatibilité xmlsec 1.2.35 (openssl 3?)

#7 - 17 novembre 2022 10:48 - Benjamin Dauvergne

J'ai réduit la branche au strict nécessaire et déplacer le reste dans d'autres tickets, si ça peut être validé.

#8 - 21 novembre 2022 10:50 - Frédéric Péters

- Statut changé de Solution proposée à Solution validée

> Uniquement 0001 donc, et je n'ai pas lu/testé les autres.

Donc la branche ramenée à 0001 c'est ok.

#9 - 21 novembre 2022 13:22 - Benjamin Dauvergne

- Statut changé de Solution validée à Résolu (à déployer)

```
commit 66ebd11166038c23e642c4f9ed2f036815872e41
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Wed Nov 16 15:35:27 2022 +0100

    Use OpenSSL EVP API to work around deprecation of low level APIs in OpenSSL 3 (#71313)

    OpenSSL API is used to sign query-string values in the SAML 2.0 Redirect binding.
    Other binding only need the libxmlsec API as signature are XML DSIG signatures.
```

#10 - 26 novembre 2023 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-wip.patch	25 ko	15 novembre 2022	Benjamin Dauvergne
0007-Fix-use-of-wrong-enumeration-NULL-value-71313.patch	869 octets	16 novembre 2022	Benjamin Dauvergne
0009-Fix-warning-about-enum-conversion-71313.patch	810 octets	16 novembre 2022	Benjamin Dauvergne
0001-Use-OpenSSL-EVP-API-to-work-around-deprecation-of-lo.patch	19,6 ko	16 novembre 2022	Benjamin Dauvergne
0010-Fix-all-cast-function-type-warnings-71313.patch	16,3 ko	16 novembre 2022	Benjamin Dauvergne
0006-Fix-warnings-about-type-casts-71313.patch	1,13 ko	16 novembre 2022	Benjamin Dauvergne
0003-Make-lasso_inflate-output-the-inflated-buffer-size-7.patch	1 ko	16 novembre 2022	Benjamin Dauvergne
0008-Fix-all-warnings-in-tests-71313.patch	106 ko	16 novembre 2022	Benjamin Dauvergne
0002-Add-new-define-LASSO_XMLSEC_VERSION_NUMBER-allow-ver.patch	1,14 ko	16 novembre 2022	Benjamin Dauvergne
0011-Fix-unused-parameters-warnings-71313.patch	1,27 ko	16 novembre 2022	Benjamin Dauvergne
0005-Replace-all-use-of-xmlSecBase64Decode-by-lasso_base6.patch	17,5 ko	16 novembre 2022	Benjamin Dauvergne
0004-Adapt-lasso_base64_decode-to-the-deprecation-of-xmlS.patch	2,25 ko	16 novembre 2022	Benjamin Dauvergne