Lasso - Development #56023

lasso_node_encrypt / hard coded PKCS#1

06 août 2021 12:31 - Stephan Schmidtmer

Statut:	Fermé	**Début:**	06 août 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:	Binding python	**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

I ran into a problem with LemonLDAP (as SAML IdP) when I tried to encrypt the assertion.
The SAML SP (SimpleSAMLphp in this case) wasn't able to decrypt it.

Cause is that SimpleSAMLphp blocks PKCS#1 by default:
https://simplesamlphp.org/docs/stable/simplesamlphp-reference-idp-remote#section_2 (encryption.blacklisted-algorithms)
Reason is probably the same as described here: http://shibboleth.net/pipermail/dev/2012-July/000858.html

I discovered that PKCS#1 for key encryption is hard coded in the function lasso_node_encrypt (lasso/xml/xml.c line 623/624):

```
    encrypted_key_node = xmlSecTmplKeyInfoAddEncryptedKey(key_info_node,
            xmlSecTransformRsaPkcs1Id, NULL, NULL, (xmlChar*)recipient);
```

If I change xmlSecTransformRsaPkcs1Id to xmlSecTransformRsaOaepId, SimpleSAMLphp happily decrypts it.

So maybe is there a change to get is configurable by a parameter?
Or some sort of logic that uses PKCS#1 for DES keys and RSA-OAEP for AES keys?

We might face this issue again in the near future when we need to add Auth0 as another SP. They probably want AES256 & RSA-OAEP:
https://auth0.com/docs/protocols/saml-protocol/saml-configuration-options/sign-and-encrypt-saml-requests#send-encrypted-saml-authentication-assertions

Révisions associées

Révision 1e718bd3 - 11 septembre 2021 19:19 - Benjamin Dauvergne

Python: fix formatting (#56023)

Révision 53b0bd35 - 11 septembre 2021 19:20 - Benjamin Dauvergne

Change default key encryption padding algorithm to RSA-OAEP (#56023)

The key encryption padding algorithm is now configurable, the default
being changed to OAEP. It's possible to set the default through
./configure with:

```
--with-default-key-encryption-method=[rsa-pkcs1|rsa-oaep]
```

at initialization time with an environment variable:

```
LASSO_DEFAULT_KEY_ENCRYPTION_METHOD=[rsa-pkcs1|rsa-oaep]
```

or at runtime for a service provider:

```
lasso_provider_set_key_encryption_method(LassoProvider *provider,
        LassoKeyEncryptionMethod key_encryption_method)
```

The setting is global for all encrypted nodes (Assertion or NameID).

Historique

#1 - 02 septembre 2021 19:53 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

It seems mandated by the specification so I will add an abstraction named "encryption_key_encryption_type" and I will change the default to OAEP..

```
# in https://www.oasis-open.org/committees/download.php/35393/sstc-saml-conformance-errata-2.0-wd-04-diff.pdf

4.2 XML Encryption Algorithms

XML Encryption mandates use of the following algorithms in Sections 5.2.1 and 5.2.2; therefore they MUST be im
plemented by compliant SAML V2.0 implementations:
* Block Encryption: TRIPLE DES, AES-128, AES-256
* Key Transport: RSA-v1.5, RSA-OAEP
```

#2 - 03 septembre 2021 12:30 - Benjamin Dauvergne

- Fichier 0002-Change-default-key-encryption-padding-algorithm-to-R.patch ajouté

- Fichier 0001-Python-fix-formatting.patch ajouté

- Tracker changé de Support à Development

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 03 septembre 2021 12:41 - Benjamin Dauvergne

- Catégorie mis à Binding python

- Assigné à changé de Benjamin Dauvergne à Stephan Schmidtmer

Could you test the given patch on your use case ?

#4 - 03 septembre 2021 17:01 - Stephan Schmidtmer

Sure, I have tested it. Looks good so far!

I applied it to 2.6.0 Debian (buster) source package, just had to manually do 3 tiny hunks.
And while the changed default to OAEP already does the trick in my case, I also verified that influencing it by the environment variable or by lasso_provider_set_key_encryption_method() is working.

Will this get into the Debian stable release package (or maybe into a backports package)?

#5 - 03 septembre 2021 17:58 - Benjamin Dauvergne

Stephan Schmidtmer a écrit :

> Will this get into the Debian stable release package (or maybe into a backports package)?

I'm not sure, there is a policy of bugfixes only I'm not sure I could backport a bugfix from this commit; there is not really a bug, but it will to testing and integrate the backports repository easily.

#6 - 06 septembre 2021 13:52 - Stephan Schmidtmer

Yes, while it can cause trouble here and there, I agree that it probably doesn't count as a bug.
But if I can get a "fixed" version as a package from the backports repository in the near future, that would be great!

#7 - 11 septembre 2021 19:20 - Benjamin Dauvergne

- Assigné à changé de Stephan Schmidtmer à Benjamin Dauvergne

#8 - 11 septembre 2021 19:20 - Benjamin Dauvergne

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

```
commit 53b0bd356982eb970581aa360d750c8a0e7132a0
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Fri Sep 3 07:48:35 2021 +0200

    Change default key encryption padding algorithm to RSA-OAEP (#56023)

    The key encryption padding algorithm is now configurable, the default
    being changed to OAEP. It's possible to set the default through
    ./configure with:

        --with-default-key-encryption-method=[rsa-pkcs1|rsa-oaep]
```

```
    at initialization time with an environment variable:

        LASSO_DEFAULT_KEY_ENCRYPTION_METHOD=[rsa-pkcs1|rsa-oaep]

    or at runtime for a service provider:

        lasso_provider_set_key_encryption_method(LassoProvider *provider,
            LassoKeyEncryptionMethod key_encryption_method)

    The setting is global for all encrypted nodes (Assertion or NameID).

commit 1e718bd3aaa4bc203c6418d3cce0e0bc1f0d19b3
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Fri Sep 3 11:13:49 2021 +0200

    Python: fix formatting (#56023)
```

#9 - 18 septembre 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0002-Change-default-key-encryption-padding-algorithm-to-R.patch	23,3 ko 03 septembre 2021	Benjamin Dauvergne
0001-Python-fix-formatting.patch	8,92 ko 03 septembre 2021	Benjamin Dauvergne