Lasso - Bug #26828

with paos response (ECP) if assertion is signed instead of response signature_not_found error occurs

29 septembre 2018 00:59 - John Dennis

Statut:	Fermé	**Début:**	29 septembre 2018
Priorité:	Normal	**Echéance:**	
Assigné à:	John Dennis	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	2.6.1		
Patch proposed:	Oui	**Planning:**	Non

Description

In SAML a signature can appear on either the top level SAML message or on an Assertion. When an Assertion is returned via a PAOS response for ECP and the signature is on the Assertion instead of on the Response an erroneous signature not found error occurs.

The problem is in lasso_saml20_login_process_paos_response_msg(). It initially calls lasso_saml20_profile_process_soap_response_with_headers() which checks for the signature on the top level SAML response. If the response is not signed it returns LASSO_DS_ERROR_SIGNATURE_NOT_FOUND. lasso_saml20_login_process_paos_response_msg() then continues to process and calls lasso_saml20_login_process_response_status_and_assertion() where it checks for the signature on the assertion. If the assertion is signed and validates it's successful. However lasso_saml20_login_process_paos_response_msg() ultimately returns the LASSO_DS_ERROR_SIGNATURE_NOT_FOUND from the earlier check on the response message when it should have realized the signature check on the assertion superseded it.

I have a git formatted patch prepared and will submit soon.

Révisions associées

Révision 642182bd - 11 janvier 2019 16:11 - John Dennis

Fix ECP signature not found error when only assertion is signed (#26828)

With a SAML Authn Response either the message or the assertion
contained in the response message or both can be signed. Most IdP's
sign the message. This fixes a bug when processing an ECP authn
response when only the assertion is signed.

lasso_saml20_profile_process_soap_response_with_headers() performs a
signature check on the SAML message. A signature can also appear on
the assertion which is checked by
lasso_saml20_login_process_response_status_and_assertion() The problem
occurred when the message was not signed and
lasso_saml20_profile_process_soap_response_with_headers() returned
LASSO_DS_ERROR_SIGNATURE_NOT_FOUND as an error code which is not
actually an error because we haven't checked the signature on the
assertion yet. We were returning the first
LASSO_DS_ERROR_SIGNATURE_NOT_FOUND error when in fact the subsequent
signature check in
lasso_saml20_login_process_response_status_and_assertion() succeeded.

The ECP unit tests were enhanced to cover these cases.

The enhanced unit test revealed a problem in two switch statements
operating on the return value of
lasso_profile_get_signature_verify_hint() which were missing a case
statement for LASSO_PROFILE_SIGNATURE_VERIFY_HINT_FORCE which caused
an abort due to an unknown enumeration value.

Fixes Bug: 26828
License: MIT
Signed-off-by: John Dennis <jdennis@redhat.com>

Historique

#1 - 29 septembre 2018 09:35 - Benjamin Dauvergne

- Assigné à mis à John Dennis

Seems legit, I'll apply it as soon as it arrives.

#2 - 09 janvier 2019 23:55 - John Dennis

- Fichier 0001-Fix-ECP-signature-not-found-error-when-only-assertio.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 10 janvier 2019 10:29 - Benjamin Dauvergne

Just add the License: MIT header and it's good.

#4 - 10 janvier 2019 15:53 - John Dennis

- Fichier 0001-Fix-ECP-signature-not-found-error-when-only-assertio.patch supprimé

#5 - 10 janvier 2019 15:54 - John Dennis

- Fichier 0001-Fix-ECP-signature-not-found-error-when-only-assertio.patch ajouté

Updated patch with MIT license tag

#6 - 19 janvier 2019 12:12 - Benjamin Dauvergne

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

#7 - 19 janvier 2019 12:12 - Benjamin Dauvergne

- Version cible mis à 2.6.1

#8 - 06 septembre 2019 14:40 - Benjamin Dauvergne

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

Fichiers

0001-Fix-ECP-signature-not-found-error-when-only-assertio.patch	10,2 ko	10 janvier 2019	John Dennis