Lasso - Bug #34409

[PAOS][ECP] lasso includes "Destination" attribute in SAML AuthnRequest populated with SP AssertionConsumerServiceURL when ECP workflow is used which leads to IdP-side errors

28 juin 2019 02:20 - Dmitrii S.

Statut:	Fermé	**Début:**	28 juin 2019
Priorité:	Haut	**Echéance:**	
Assigné à:	John Dennis	**% réalisé:**	100%
Catégorie:	SAMLv2	**Temps estimé:**	0:00 heure
Version cible:	2.6.1		
Patch proposed:	Oui	**Planning:**	Non

Description

Downstream bug:
https://bugs.launchpad.net/ubuntu/+source/lasso/+bug/1833299

Lasso is used by libapache2-mod-auth-mellon to create SAML messages. When ECP profile (http://docs.oasis-open.org/security/saml/Post2.0/saml-ecp/v2.0/cs01/saml-ecp-v2.0-cs01.pdf) is used with PAOS binding Lasso populates an AuthnRequest with the "Destination" attribute as follows:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="
urn:oasis:names:tc:SAML:2.0:assertion" ID="_798F26F73776E684A463559CDB77D080" Version="2.0"
IssueInstant="2019-06-18T16:54:25Z" Destination="
https://keystone.maas:5000/v3/OS-FEDERATION/identity_providers/samltestid/protocols/saml2/auth/mel
lon/paosResponse" Consent="urn:oasis:names:tc:SAML:2.0:consent:current-implicit" SignType="0"
SignMethod="0" ForceAuthn="false" IsPassive="false" AssertionConsumerServiceURL="
https://keystone.maas:5000/v3/OS-FEDERATION/identity_providers/samltestid/protocols/saml2/auth/mel
lon/paosResponse">
    <saml:Issuer>
https://keystone.maas:5000/v3/OS-FEDERATION/identity_providers/samltestid/protocols/saml2/auth
</saml:Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">

...
```

This triggers the IdP-side Destination attribute validation logic relevant explicitly for "HTTP Redirect" and "HTTP POST" bindings only (per the spec, sections 3.4.5.2 and 3.5.5.2), not the PAOS binding (a section before 3.4). Practically, it seems like this logic makes sense to use for any binding that uses a client as a means of transporting a request and does not allow a client to select an IdP.
http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

For example, Shibboleth IdP (samltest.id) errors out as follows as the Destination attribute was populated with an SP URL:

```
2019-06-18 16:54:25,435 - ERROR [org.opensaml.saml.common.binding.security.impl.ReceivedEndpointSe
curityHandler:?] - Message Handler: SAML message intended destination endpoint 'https://keystone.m
aas:5000/v3/OS-FEDERATION/identity_providers/samltestid/protocols/saml2/auth/mellon/paosResponse'
did not match the recipient endpoint 'https://samltest.id/idp/profile/SAML2/SOAP/ECP'
```

The profiles spec says that ECP determines the IdP and Mellon documentation refers to the same (https://git.io/fjVIz):
http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
"4.2.2 Profile Overview ...
3. ECP determines Identity Provider to use (methods vary, details not shown)"

"Destination" is marked as optional in the schema and I tested that Shibboleth (samltest.id) does not error out when it is not present with ECP+PAOS workflow:
https://docs.oasis-open.org/security/saml/v2.0/saml-schema-protocol-2.0.xsd

I also analyzed the code of Keycloak and it seems that it will have exactly the same logic of ignoring the absence of a Destination attribute if it is not present and erroring out when it is set to an SP assertion consumer URL.
https://github.com/keycloak/keycloak/blob/6.0.1/saml-core/src/main/java/org/keycloak/saml/validators/DestinationValidator.java#L82-L101

So for PAOS/ECP it makes sense to avoid the inclusion of the "Destination" attribute to AuthnRequest.

As a side example, Shibboleth SP's PAOS/ECP implementation does not include this attribute based on what I can see in this post http://idmoim.blogspot.com/2015/02/

The patch attached was tested on with:

- mellon 0.14.2 (0.14.2-1ubuntu1);
- Keystone (Queens) as an ECP client;
- samltest.id as an IdP (Shibboleth IdP 3.x);
- lasso 2.5.1 (with the patch applied).

Test results:

openstack client (ECP) log for `openstack token issue`: https://paste.ubuntu.com/p/SQJFjNGx7k/
Mellon diagnostics log: https://paste.ubuntu.com/p/SqyZT8QCNb/
IdP (samltest.id) log: https://paste.ubuntu.com/p/DZszPPf4Bs/

Distro build log: https://paste.ubuntu.com/p/PP4TVKdGsF/

Révisions associées

Révision 77c0bc86 - 03 juillet 2019 20:04 - Dmitrii Shcherbakov

PAOS: Do not populate "Destination" attribute

When ECP profile (saml-ecp-v2.0-cs01) is used with PAOS binding Lasso
populates an AuthnRequest with the "Destination" attribute set to
AssertionConsumerURL of an SP - this leads to IdP-side errors because
the destination attribute in the request does not match the IdP URL.

The "Destination" attribute is mandatory only for HTTP Redirect and HTTP
Post bindings when AuthRequests are signed per saml-bindings-2.0-os
(sections 3.4.5.2 and 3.5.5.2). Specifically for PAOS it makes sense to
avoid setting that optional attribute because an ECP decides which IdP
to use, not the SP.

Fixes #34409

Signed-off-by: Dmitrii Shcherbakov <dmitrii.shcherbakov@canonical.com>

Historique

#1 - 28 juin 2019 10:32 - Benjamin Dauvergne

- Assigné à mis à John Dennis

It seems ok but I'm not the more knowledgeable person on the ECP binding, I attribute the ticket to John Dennis for review.

#2 - 28 juin 2019 10:37 - Benjamin Dauvergne

Instead of doing an assign_string(.., NULL) you can do a lasso_release_string(...), it also reset the target to NULL and is more idiomatic in Lasso.

#3 - 28 juin 2019 11:06 - Dmitrii S.

- Fichier 0001-PAOS-Do-not-populate-Destination-attribute.patch ajouté

Benjamin Dauvergne a écrit :

> Instead of doing an assign_string(.., NULL) you can do a lasso_release_string(...), it also reset the target to NULL and is more idiomatic in Lasso.

Thanks for triaging and the review.

Updated the patch and retested.

Will wait for feedback from John.

#4 - 02 juillet 2019 00:00 - John Dennis

The analysis was well done, Dmitri correctly identified the root cause, the Destination attribute should not be set when generating an AuthnRequest to be transported via PAOS.

However, I have nits with the proposed patch part of which has to do with the code legacy in lasso. It is unfortunate that lasso_saml20_profile_build_request_msg() takes a url parameter which is obstinately used to the the msg_url (i.e. the receiver of the message). That's fine for many of the SAML profiles but it's not for ECP. ECP has a different requirement, it needs to set the responseConsumerURL attribute in the paos:Request element to the AssertionConsumerServiceURL. Because the existing function signatures (lasso_saml20_profile_build_request_msg() and lasso_saml20_profile_build_*_msg() variants) did not allow for drawing a distinction between the msg_url and an assertionConsumerServiceURL **and** because lasso_saml20_profile_build_request_msg() demanded a url (or it would pick one), the url parameter was abused. For PAOS the url parameter was set to the assertionConsumerServiceURL so that it could eventually populate the paos:responseConsumerURL via the call to lasso_node_export_to_paos_request_full(). That's the history, but to make things cleaner would require a bit of refactoring, we don't need to refactor now to fix this, just pointing out it might be worthwhile down the road.

Given the above I would recommend removing the added comment in lasso_saml20_login_build_authn_request_msg which discusses the destination attribute, it's just confusing matters because this is not the part of the code that is dealing with the issue. If any comment needs to be added here it probably would be better to comment on the abuse of the url parameter. The only other change in lasso_saml20_login_build_authn_request_msg() aside from the comment is renaming the local variable "url" to "consumer_url". I'm good with that, it's always better to be explicit (url is way too generic). However my suggestion would be to maintain consistency with the existing naming practice and call the local variable "assertionConsumerServcieURL" as is done elsewhere.

The actual fix is in lasso_saml20_profile_build_request_msg(), the comment is good but setting the Destination attribute to NULL might be more appropriately done with lasso_release_string(xxx) as opposed to lasso_assign_string(xxx, NULL), I don't think there are any existing examples of using lasso_assign_string() with NULL (it should work fine). But that is a nit I'll leave up to Benjamin as to what he prefers for code consistency.

Thank you for the excellent bug report Dmitri and careful analysis, it is much appreciated.

#5 - 03 juillet 2019 08:20 - Dmitrii S.

- Fichier 0001-PAOS-Do-not-populate-Destination-attribute.patch ajouté

John,

Thanks a lot for the prompt reply, code review and prior work across the stack.

> That's the history, but to make things cleaner would require a bit of refactoring, we don't need to refactor now to fix this, just pointing out it might be worthwhile down the road.

I agree that an API redesign might take a significant amount of time and thought while a more tactical fix will solve the problem without that, especially considering that it will be easier to backport a small fix back to older versions of lasso at the distribution level and unblock users in terms of using ECP.

I addressed the review in the 3rd iteration of the patch uploaded with this message. I agree that extra comments are not necessary in lasso_saml20_login_build_authn_request_msg and that variable naming should be consistent with everything else. I added a reference to this bug in a comment in the code for context though.

lasso_release_string is now also used in lasso_saml20_profile_build_request_msg.

#6 - 03 juillet 2019 20:04 - Anonyme

- Statut changé de Nouveau à Résolu (à déployer)

- % réalisé changé de 0 à 100

Appliqué par commit 77c0bc86058e3d83042dac9e8297e2a571ed4da6.

#7 - 03 juillet 2019 20:07 - Benjamin Dauvergne

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

I reverted my push; Dmitrii could you add a License: MIT header to the bottom of your patch to state that you contributed (and Canonical your employer) under the MIT license ? We do dual licensing on Lasso and we need that for external contributors.

#8 - 03 juillet 2019 21:31 - Dmitrii S.

- Fichier 0001-PAOS-Do-not-populate-Destination-attribute.patch ajouté

Benjamin Dauvergne a écrit :

> I reverted my push; Dmitrii could you add a License: MIT header to the bottom of your patch to state that you contributed (and Canonical your employer) under the MIT license ? We do dual licensing on Lasso and we need that for external contributors.

Sure, added the inbound license.

Btw (just curious), is there a public contribution policy doc for lasso?

#9 - 03 juillet 2019 23:53 - Benjamin Dauvergne

Dmitrii S. a écrit :

> Benjamin Dauvergne a écrit :
>
> > I reverted my push; Dmitrii could you add a License: MIT header to the bottom of your patch to state that you contributed (and Canonical your employer) under the MIT license ? We do dual licensing on Lasso and we need that for external contributors.
>
> Sure, added the inbound license.
>
> Btw (just curious), is there a public contribution policy doc for lasso?

Not really, we need a permissive license for external contributions so that we can relicense as we want, but the public distribution license is GPL v2 or later.

#10 - 03 juillet 2019 23:59 - Benjamin Dauvergne

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

```
commit 1e85f1b2bd30c0d93b4a2ef37b35abeae3d15b56 (HEAD -> master, origin/master, origin/HEAD)
Author: Dmitrii Shcherbakov <dmitrii.shcherbakov@canonical.com>
Date:   Fri Jun 28 02:36:19 2019 +0300

    PAOS: Do not populate "Destination" attribute

    When ECP profile (saml-ecp-v2.0-cs01) is used with PAOS binding Lasso
    populates an AuthnRequest with the "Destination" attribute set to
    AssertionConsumerURL of an SP - this leads to IdP-side errors because
    the destination attribute in the request does not match the IdP URL.

    The "Destination" attribute is mandatory only for HTTP Redirect and HTTP
    Post bindings when AuthRequests are signed per saml-bindings-2.0-os
    (sections 3.4.5.2 and 3.5.5.2). Specifically for PAOS it makes sense to
    avoid setting that optional attribute because an ECP decides which IdP
    to use, not the SP.

    Fixes Bug: 34409
    License: MIT
    Signed-off-by: Dmitrii Shcherbakov <dmitrii.shcherbakov@canonical.com>
```

#11 - 03 septembre 2019 13:48 - Benjamin Dauvergne

- Version cible changé de future à 2.6.1

#12 - 06 septembre 2019 14:40 - Benjamin Dauvergne

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

Fichiers

0001-PAOS-Do-not-populate-Destination-attribute.patch	4,36 ko	27 juin 2019	Dmitrii S.
0001-PAOS-Do-not-populate-Destination-attribute.patch	4,37 ko	28 juin 2019	Dmitrii S.
0001-PAOS-Do-not-populate-Destination-attribute.patch	4,08 ko	03 juillet 2019	Dmitrii S.
0001-PAOS-Do-not-populate-Destination-attribute.patch	4,09 ko	03 juillet 2019	Dmitrii S.