Lasso - Bug #56492

SAML response replay is possible in some cases

30 août 2021 17:34 - Evgenii Kosov

Statut:	Fermé	**Début:**	30 août 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Evgenii Kosov	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

The lasso_saml20_login_accept_sso function has anti replay protection, which seems to be generating false negatives in some situations.
As a result I'm able to call lasso_saml20_login_process_authn_response_msg() and lasso_saml20_login_accept_sso() twice for the same SAML response within the same session and get a successful result code, which is NOT expected.

I'm willing to disclose a PoC for the issue upon request from Lasso developers.

Historique

#1 - 04 septembre 2021 11:02 - Benjamin Dauvergne

- Assigné à mis à Evgenii Kosov

Real replay protection MUST be handled by the callers as it must be done against the current time and timestamp on the response and assertions anyway. Lasso is made to be stateless and does not provide any security based on statefull properties (it's usually done by storing assertions/response IDs in a database with timestamps). What's implemented inside accept_sso is a toy replay protection; but I would still be happy to see your PoC here.

#2 - 28 mars 2022 09:59 - Pierre Cros

- Priorité changé de Haut à Normal

#3 - 28 mars 2022 10:45 - Benjamin Dauvergne

- Statut changé de Nouveau à Fermé