Lasso - Support #51350

Where to report Security Issues

22 février 2021 20:35 - Victor Schönfelder

Statut:	Fermé	**Début:**	22 février 2021
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:	SAMLv2	**Temps estimé:**	0:00 heure
Version cible:	2.6.2		
Patch proposed:	Non	**Planning:**	Non

Description

Hello,
what is the preferred place to report possible Security Issues in Lasso?
Thank you in advance

Historique

#1 - 22 février 2021 20:39 - Frédéric Péters

Hi! You can send me an email at fpeters@entrouvert.com, my PGP ID is 7149 147D F2F4 6AE0 3D55 6E3B 2AE9 01E5 C702 18D2.

#2 - 23 février 2021 12:39 - Benjamin Dauvergne

Weakness: XML Node Splitting

There is no security problem here, users of the Lasso library are expected to iterate the LassoMiscTextNode from the AttributeValue.any linked list to build the full string value, see for example https://git.entrouvert.org/django-mellon.git/tree/mellon/views.py#n217

Weakness: Processing multiple Assertions

It's not possible to add assertions as the Response is always signed also and anyway no IdP ever sent multiple assertions in production and no client I know about expected it, so it's not a real problem either (they would just be ignored). And when using the "Artifact" binding, it's not even possible to intercept AuthnResponse and modify them.

In the grand scheme of thing XMLSEC is an abomination anyway that provide only fake security. See https://www.cs.auckland.ac.nz/~pgut001/pubs/xmlsec.txt for a full report on it.

PS: the objection about signature on the AuthnResponse also apply to the first weakness, you will not be able to modify the response.

#3 - 23 février 2021 12:39 - Benjamin Dauvergne

- Statut changé de Nouveau à Fermé