Authentic 2 - Bug #60841

SAML2 - Internal Server Error à la connexion

19 janvier 2022 16:59 - Benjamin Renard

Statut:	Fermé	**Début:**	19 janvier 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Renard	**% réalisé:**	0%
Catégorie:	SAML	**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Sur notre instance d'Authentic2 de demo (version *3.69-1~eob100+1*, dernière dispo pour Buster), on a une erreur 500 suite à une connexion SAML2 à priori réussie vu où l'erreur se situe dans le code :

```
176.159.32.89 Admins Easter-eggs r:7F7056B0AE10 ERROR Internal Server Error: /idp/saml2/sso
                                        Traceback (most recent call last):
                                          File "/usr/lib/python3/dist-packages/django/core/handler
s/exception.py", line 41, in inner
                                            response = get_response(request)
                                          File "/usr/lib/python3/dist-packages/django/core/handler
s/base.py", line 187, in _get_response
                                            response = self.process_exception_by_middleware(e, req
uest)
                                          File "/usr/lib/python3/dist-packages/django/core/handler
s/base.py", line 185, in _get_response
                                            response = wrapped_callback(request, *callback_args, *
*callback_kwargs)
                                          File "/usr/lib/python3/dist-packages/authentic2/decorato
rs.py", line 47, in f
                                            return func(request, *args, **kwargs)
                                          File "/usr/lib/python3/dist-packages/authentic2/decorato
rs.py", line 47, in f
                                            return func(request, *args, **kwargs)
                                          File "/usr/lib/python3/dist-packages/django/views/decora
tors/cache.py", line 57, in _wrapped_view_func
                                            response = view_func(request, *args, **kwargs)
                                          File "/usr/lib/python3/dist-packages/django/views/decora
tors/csrf.py", line 58, in wrapped_view
                                            return view_func(*args, **kwargs)
                                          File "/usr/lib/python3/dist-packages/authentic2/idp/saml
/saml2_endpoints.py", line 155, in f
                                            return func(request, *args, **kwargs)
                                          File "/usr/lib/python3/dist-packages/authentic2/idp/saml
/saml2_endpoints.py", line 629, in sso
                                            return sso_after_process_request(request, login, nid_f
ormat=nid_format)
                                          File "/usr/lib/python3/dist-packages/authentic2/idp/saml
/saml2_endpoints.py", line 954, in sso_after_process_request
                                            name_id = build_assertion(request, login, provider, ni
d_format=nid_format)
                                          File "/usr/lib/python3/dist-packages/authentic2/idp/saml
/saml2_endpoints.py", line 467, in build_assertion
                                            fill_assertion(request, login.request, assertion, logi
n.remoteProviderId, nid_format)
                                          File "/usr/lib/python3/dist-packages/authentic2/idp/saml
/saml2_endpoints.py", line 209, in fill_assertion
                                            assertion.subject.nameID.content = transient_id_conten
t
                                        AttributeError: 'NoneType' object has no attribute 'conten
t'
```

Note : on utilise votre version *2.7.0-1~eob100+1* de *liblasso3* et *python3-lasso*. J'ai tenté de passer sur la version *2.6.0-2+deb10u1*,

mais ça change rien.

Pour info, voilà ce que donne un *assertion.dump()* juste avant la ligne problématique :

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" ID="_E70C503C8F73
64EF4383DD0EC3079B9B" IssueInstant="2022-01-19T15:52:07Z" SignType="0" SignMethod="0" EncryptionAc
tivated="false" EncryptionSymKeyType="0"><saml:Issuer>https://auth.demo.easter-eggs.com/idp/saml2/
metadata</saml:Issuer><Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                                        <SignedInfo>
                                        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/
10/xml-exc-c14n#"/>
                                        <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmld
sig-more#rsa-sha256"/>
                                        <Reference URI="#_E70C503C8F7364EF4383DD0EC3079B9B">
                                        <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#en
veloped-signature"/>
                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c1
4n#"/>
                                        </Transforms>
                                        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#
sha256"/>
                                        <DigestValue/>
                                        </Reference>
                                        </SignedInfo>
                                        <SignatureValue/>
                                        <KeyInfo>
                                        <X509Data/>
                                        </KeyInfo>
                                        </Signature><saml:Subject><saml:EncryptedID><EncryptedData
 xmlns="http://www.w3.org/2001/04/xmlenc#" Type="http://www.w3.org/2001/04/xmlenc#Element">
                                        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xml
enc#aes128-cbc"/>
                                        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                                        <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#" Re
cipient="https://ldap.demo.easter-eggs.com/">
                                        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xml
enc#rsa-1_5"/>
                                        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                                        <X509Data>
                                        <X509Certificate>MIICzzCCAbcCFCHoN7CLm93WwfF4gPnrYqswPGAaM
A0GCSqGSIb3DQEBCwUAMCQx
                                        IjAgBgNVBAMMGWxkYXAuZGVtby5lYXN0ZXItZWdncy5jb20wHhcNMjIwMT
E0MTcz
                                        MTAwWhcNMzIwMTE0MTczMTAwWjAkMSIwIAYDVQQDDBlsZGFwLmRlbW8uZW
FzdGVy
                                        LWVnZ3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmr
YkMS4I
                                        QgvPM8IW3jHywJFLZwAQu3i0cRCU9e6g0ZneIGFdhe8aSZ+NNGUDiFS3oT
1QKGLL
                                        RzBwB4KeIKQr0v590onu0Jfj/KQLfQMYvm/n5kD9tf+U5kh9ZdxKyzd65P
a75z1l
                                        D7t152XcOEvaOdIpWuUnYiZlPV49C03A/QGGwMXASq3JngsAA55d+bpt5g
o7WJOX
                                        as1pS+s2+V+9On1ww4Rridu82mr+cGUHuigpINNXdsvaOoPPuhX/0gR/Wi
gTJ0Ug
                                        FXPX74AFMQ/D9NjjZWYWAaSVeRLgpReVvxa/lJXHIaGcDAFgXhkzi//DBh
NnSTaC
                                        ktQqlRVvcVP/KwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBsjl6CmFcZae
KpMpe4
                                        klLaPXLXLzHJJsb5NClkyTk1TPBALf9BsNzeiwPJ0u44oANSl75meCxCkx
D6tMCw
                                        hhIV0Cgh6FQLGKwV71IhrAtD5l2TvU/ZQ2LjxpiV6sg4JQ0qAAX7ddP3CE
f9Cb3u
                                        pC70JyiZulqxj/NLifaDlfLmc5HcJjGhzZGdGQjpjtAHaIq6yP3LCwgzPi
yyw1y3
                                        dyQuw4ebzJIgNHXxt98V20X9C3qATAZdgkRPJ5NlgAmibDmAU4NQrtDRWL
```

```
UjQu/Z
                                        r7+kfKanTk9aZ6X6gT1ruECNA2j4slJhZYrLBY+HnrLJ3c+5rmI2CKYTh9
T6cI8R
                                        C5tf</X509Certificate>
                                        </X509Data>
                                        </KeyInfo>
                                        <CipherData>
                                        <CipherValue>Hvni7VNvcjTW+WxuFBqon7MCq2PHGyHC8XQ6NbGDs4IoK
DW0HAF2XDrOB2l9u2b4
                                        i4JjS9ZvDqMLXRexpz2pmJfwbGuuXmI/GeljSX0UAXOBrhbc9CsVbxjrwO
vLVKgR
                                        davUK3avMBi9NDOsYHUC0A4elYmdExoLiJSiFin+EcaOtwKJMOeo3VHzSv
jW45Pn
                                        dH4/AZXpM+wTWYGNsfDRUUKM+TTKWVHd9Jw+zX/gpiQ2zCGbtTwZVlZH5N
52sgho
                                        0ZvHDtO/Hp3TR4zMB8ZQwqwqDlgMysk8VzrRb9TtH6x3fC2zZWjyXEuO1J
Z4GYDc
                                        YKEagHvXS6qR6Sp4nwE/zQ==</CipherValue>
                                        </CipherData>
                                        </EncryptedKey>
                                        </KeyInfo>
                                        <CipherData>
                                        <CipherValue>Tic6MPxhjTzuurvY6gqDFAC/6R5QSn75suC9+0VBwT6XD
h8ucW1tyrOzqfTr8vkD
                                        YMEqq2+pfPLZVivfBpklzWlaqWYd3iQGGiZctywWuHW8RIr1YL+u7rDwFl
S6ZKVL
                                        gnV1NJiTURJRE9UtQjminpR0wiAGbdIJSFSuftExeOHRsIwTFrIskSbEKa
8SOCTI
                                        KHXu4yrY8eXXT/LeaSZLyOUgAA4ueKtepkjeMqjOGUeqVUtyB30ODds5mn
59EsgT
                                        m9yDmIFpA98UAr7+n+ykejZliyKF4qqYP+/IbEQGTRdKJBDZtVFVIiieBg
FSYzL+
                                        WMu1zN7T9nQ5Ube9cx0HvPwJWYNpbaco3Gprk4BjhhY=</CipherValue>
                                        </CipherData>
                                        </EncryptedData><saml:NameID Format="urn:oasis:names:tc:SA
ML:2.0:nameid-format:transient" NameQualifier="https://auth.demo.easter-eggs.com/idp/saml2/metadat
a">_FF8DC553BF49A24B4430F010397799CA</saml:NameID></saml:EncryptedID><saml:SubjectConfirmation Met
hod="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData NotOnOrAfter="2022-01-19
T15:53:07.273195Z" InResponseTo="_CC4AFF05FB14CA9FEE944E632A66E8B3"/></saml:SubjectConfirmation></
saml:Subject><saml:Conditions NotBefore="2022-01-19T15:51:07.273195Z" NotOnOrAfter="2022-01-19T15:
53:07.273195Z"><saml:AudienceRestriction><saml:Audience>https://ldap.demo.easter-eggs.com/</saml:A
udience></saml:AudienceRestriction></saml:Conditions><saml:AuthnStatement AuthnInstant="2022-01-19
T15:52:07.273195Z" SessionIndex="_E70C503C8F7364EF4383DD0EC3079B9B" SessionNotOnOrAfter="2022-01-1
9T21:52:07Z"><saml:AuthnContext><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:
Password</saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement></saml:Assertion>
```


Historique

#1 - 26 janvier 2022 18:14 - Benjamin Dauvergne

- Statut changé de Nouveau à Information nécessaire

- Assigné à mis à Benjamin Renard

Je n'ai aucune idée du problème mais on voit un NameID chiffré dans le dump en plus de sa version déchiffrée, il faudrait voir pourquoi il est chiffré et si ça n'interagit pas difficilement avec le mode transient_id.

#2 - 26 janvier 2022 19:22 - Benjamin Dauvergne

À la lecture du code de Lasso je confirme que la combinaison du chiffrement du NameID et de sa modification après lasso_login_build_assertion() ne marche juste pas, c'est incompatible.

#3 - 27 janvier 2022 18:42 - Benjamin Renard

Benjamin Dauvergne a écrit :

> À la lecture du code de Lasso je confirme que la combinaison du chiffrement du NameID et de sa modification après lasso_login_build_assertion() ne marche juste pas, c'est incompatible.

Ça ressemble donc à un bug côté Authentic, tu confirmes ? Merci en tout cas pour ton analyse !

#4 - 27 janvier 2022 18:46 - Benjamin Dauvergne

Benjamin Renard a écrit :

> Benjamin Dauvergne a écrit :
>
> > À la lecture du code de Lasso je confirme que la combinaison du chiffrement du NameID et de sa modification après lasso_login_build_assertion() ne marche juste pas, c'est incompatible.
>
> Ça ressemble donc à un bug côté Authentic, tu confirmes ? Merci en tout cas pour ton analyse !

Non authentic n'y est pour rien, c'est Lasso qui ne propose aucune moyen à Authentic pour faire ça, le seul moyen d'éviter la 500 ce serait de retourner une erreur propre disant que l'action demandée est impossible.

#5 - 27 janvier 2022 19:13 - Benjamin Renard

Benjamin Dauvergne a écrit :

> Non authentic n'y est pour rien, c'est Lasso qui ne propose aucune moyen à Authentic pour faire ça, le seul moyen d'éviter la 500 ce serait de retourner une erreur propre disant que l'action demandée est impossible.

OK. En face, c'était un bête *mod_mellon* (version *0.16.0-1~bpo10+1*) et je viens de repasser sur la version Buster (*0.14.2-1*) et ça règle le problème à priori. En Bullseye, c'est une version un peu plus récente (*0.17.0-1*) : j'espère qu'elle n'a pas le même comportement, car on serait mal.

#6 - 27 janvier 2022 19:58 - Benjamin Dauvergne

Il faut vérifier les métadonnées du mod_mellon, s'il demande à chiffrer les NameID par défaut maintenant, ça reste configurable.

#7 - 22 février 2022 19:14 - Benjamin Dauvergne

- Statut changé de Information nécessaire à Solution déployée

Je pense que ça vient entièrement d'une configuration particulière, pas de la version de modmellon, un diff entre la 0.16 et la 0.17 ne m'a montré aucune différence particulière niveau chiffrement des assertions.

#8 - 24 avril 2022 04:42 - Transition automatique

Automatic expiration