Lasso - Development #54689

Dead code after the recent CVE patch

09 juin 2021 10:16 - Jakub Hrozek

Statut:	Fermé	**Début:**	09 juin 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

I ran the recent CVE patch through Coverity and Coverity found out that there is unreachable code in lasso_saml20_login_process_response_status_and_assertion.

This part:

```
        switch (verify_hint) {
                case LASSO_PROFILE_SIGNATURE_VERIFY_HINT_FORCE:
                case LASSO_PROFILE_SIGNATURE_VERIFY_HINT_MAYBE:
                        break;
                case LASSO_PROFILE_SIGNATURE_VERIFY_HINT_IGNORE:
                        /* ignore signature errors */
                        if (rc == LASSO_PROFILE_ERROR_CANNOT_VERIFY_SIGNATURE) {
                                rc = 0;
                        }
                        break;
                default:
                        g_assert(0);
        }
```

rc is only ever assigned to here:

```
                        if (lasso_strisnotequal(in_response_to,login->private_data->request_id)) {
                                rc = LASSO_LOGIN_ERROR_ASSERTION_DOES_NOT_MATCH_REQUEST_ID;
                                goto cleanup;
                        }
```

and the rc value can therefore never be LASSO_PROFILE_ERROR_CANNOT_VERIFY_SIGNATURE.

I'm unsure what the code was supposed to do there? Reading the code seems correct to me as if the signature validation fails, the code is always ignored, but I'm unsure if the condition on 1440:

```
»·····»·····if (profile->signature_status != 0) {
»·····»·····»·····/* When response signature is not present */
»·····»·····»·····if (verify_hint == LASSO_PROFILE_SIGNATURE_VERIFY_HINT_MAYBE) {
»·····»·····»·····»·····assertion_signature_status =
»·····»·····»·····»·····»·····lasso_saml20_login_check_assertion_signature(login, assert
ion);
»·····»·····»·····»·····if (assertion_signature_status) {
»·····»·····»·····»·····»·····goto_cleanup_with_rc(assertion_signature_status);
»·····»·····»·····»·····}
»·····»·····»·····}
```

is also supposed to handle HINT_FORCE?

Sorry I'm not contributing a patch, but this code seems complex and I still don't know my way around lasso well enough.

Révisions associées

Révision 2d786348 - 23 novembre 2022 09:40 - Jakub Hrozek

In lasso_saml20_login_process_response_status_and_assertion remove dead switch (#54689)

In case VERIFY_HINT was set to IGNORE and the login signature was
incorrect, lasso_saml20_login_process_response_status_and_assertion
would have jumped straight to the cleanup label which just returns the
return code.

Related: https://dev.entrouvert.org/issues/54689
License: MIT

Révision 16148102 - 23 novembre 2022 09:40 - Benjamin Dauvergne

In lasso_saml20_login_process_response_status_and_assertion does not overwirte signature_status with rc which is always at 0 (#54689)

We are losing information in this case, like if the response was not
signed.

Historique

#1 - 24 juin 2021 02:32 - Benjamin Dauvergne

Yeah it became complex :

- if message lacks signature (signature_status == SIGNATURE_NOT_FOUND and hint is FORCE, we abort
- if signature element present but does not validate, for any hint

What I see know is that we made SIGNATURE_IGNORE not working anymore when a signature does not check, only if signature are absent (I'm not sure it's really a problem).

So later if signature_status is != 0 it means that hint is not force but IGNORE or MAYBE, FORCE is impossible now.

That's for you last remark.

Concerning the switch, yes it is dead since all handling of the different verify_hint values is done before and they are a lot more strict, an existing <Signature> cannot be ignored anymore.

#2 - 24 juin 2021 23:07 - Jakub Hrozek

Thank you for your answer. It seems like mellon has an option to ignore the broken signature on logout (added by you :-)) that uses LASSO_PROFILE_SIGNATURE_VERIFY_HINT_IGNORE so for mellon in RHEL, I would prefer to fix that option one way or another.

Would you prefer me to send a patch or would you prefer to do it since the code is security sensitive?

#3 - 05 juillet 2021 11:25 - Jakub Hrozek

oh, I finally re-read both the lasso code more carefully and the mellon code as well and only now realized that the mellon code only uses the ignore hint on logout.

I agree with you that this issue is not really worth fixing, then, ignoring signatures on login seems like something that shouldn't even be done :-)

Thank you for your reply.

#4 - 05 juillet 2021 11:52 - Jakub Hrozek

- Fichier 0001-lasso_saml20_login_process_response_status_and_asser.patch ajouté

A minimal proposed patch. I'm unsure if this should be fixed, though.

#5 - 26 juillet 2021 16:28 - Jakub Hrozek

- Fichier 0001-lasso_saml20_login_process_response_status_and_asser.patch ajouté

Probably a safer patch after some discussion with Simo, getting rid of the switch and just explicitly handling IGNORE in the existing cleanup handlers.

#6 - 27 juillet 2021 14:12 - Jakub Hrozek

- Fichier 0001-lasso_saml20_login_process_response_status_and_asser.patch ajouté

OK, one more try, this time rebased on the proper branch and without an unitialized variable warning...

#7 - 17 novembre 2022 10:46 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#8 - 17 novembre 2022 10:46 - Benjamin Dauvergne

- Fichier 0001-In-lasso_saml20_login_process_response_status_and_as.patch ajouté

- Fichier 0002-In-lasso_saml20_login_process_response_status_and_as.patch ajouté

- Tracker changé de Bug à Development

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

I finnally had time to review your code, I think that the line added to cleanup are not needed since, we chose consciously to to not ignore invalid signatures on Response even in the IGNORE case during the correction for the last CVE. But I also removed code to not overwirte profile->signature_status in this case.

#9 - 17 novembre 2022 21:20 - Benjamin Dauvergne

- Fichier 0001-In-lasso_saml20_login_process_response_status_and_as.patch ajouté

- Fichier 0002-In-lasso_saml20_login_process_response_status_and_as.patch ajouté

#10 - 18 novembre 2022 10:02 - Serghei Mihai

- Statut changé de Solution proposée à Solution validée

#11 - 23 novembre 2022 09:40 - Benjamin Dauvergne

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

```
commit 16148102e5e35262ac9536b1f2cf4a2370731466
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Nov 17 10:43:34 2022 +0100

    In lasso_saml20_login_process_response_status_and_assertion does not overwirte signature_status with rc wh
ich is always at 0 (#54689)

    We are losing information in this case, like if the response was not
    signed.

commit 2d7863482750891e11d5baa6d612235c6b52055c
Author: Jakub Hrozek <jhrozek@redhat.com>
Date:   Mon Jul 26 16:25:52 2021 +0200

    In lasso_saml20_login_process_response_status_and_assertion remove dead switch (#54689)

    In case VERIFY_HINT was set to IGNORE and the login signature was
    incorrect, lasso_saml20_login_process_response_status_and_assertion
    would have jumped straight to the cleanup label which just returns the
    return code.

    Related: https://dev.entrouvert.org/issues/54689
    License: MIT
```

#12 - 26 novembre 2023 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-lasso_saml20_login_process_response_status_and_asser.patch	1,58 ko	05 juillet 2021	Jakub Hrozek
0001-lasso_saml20_login_process_response_status_and_asser.patch	1,6 ko	26 juillet 2021	Jakub Hrozek
0001-lasso_saml20_login_process_response_status_and_asser.patch	2,04 ko	27 juillet 2021	Jakub Hrozek
0001-In-lasso_saml20_login_process_response_status_and_as.patch	1,76 ko	17 novembre 2022	Benjamin Dauvergne
0002-In-lasso_saml20_login_process_response_status_and_as.patch	1,05 ko	17 novembre 2022	Benjamin Dauvergne
0001-In-lasso_saml20_login_process_response_status_and_as.patch	1,76 ko	17 novembre 2022	Benjamin Dauvergne
0002-In-lasso_saml20_login_process_response_status_and_as.patch	1,05 ko	17 novembre 2022	Benjamin Dauvergne