ESUP-2014-AVI-002 - Vulnérabilité dans uPortal

Utilisation et diffusion de ce document

Les avis de sécurité du consortium ESUP-Portail portent sur des vulnérabilités des logiciels diffusés par le consortium. Il est de la responsabilité de chacun des destinataires de ce document de ne pas le redifuser en dehors du cadre pour lequel il a été écrit, pour des raisons évidentes de sécurité des Systèmes d'Information de tous les établissements du consortium ESUP-Portail.

Objet	Vulnérabilité dans uPortal
Référence	ESUP-2014-AVI-002
Date de la première version	26 août 2014
Date de la dernière version	26 août 2014
Source	liste de diffusion uportal-user du consortium JASIG
Diffusion de cette version	Publique
Historique	• 21 août 2014 : réception de la faille CVE-2014-5059 sur uportal-user • 25 août 2014 : prise en compte et validation de la faille sur un uPortal V4 (Pascal Rigaux) • 25 août 2014 : validation de la solution proposée sur un uPortal V4 (Pascal Rigaux) • 26 août 2014 : rédaction de la première version de cet avis (Vincent Bonamy, Pascal Rigaux) • 26 août 2014 : mise en ligne d'un correctif pour le packaging EsupV4 -> uportal-4.0.15-esup-1 (Vincent Bonamy) • 26 août 2014 : envoi de l'avis de sécurité à securite@esup-portail.org • 03 sept 2014 : envoi de l'avis de sécurité à esup-utilisateurs@esup-portail.org
Planning prévisionnel	-
Pièces jointes	-

Risque

- **Usurpation d'identité** : n'importe quel utilisateur connecté peut s'authentifier sur l'ensemble de l'ENT (socle et portlets associées) sous le compte d'une autre personne.
- Récupération et modification d'informations personnelles par un autre utilisateur connecté ; selon les services inclus directement dans le socle : mails, espace de stockage, dossier personnel, ...
- La connexion en tant qu'admin dans l'ENT et modification de celui-ci est donc possible en connaissant le login d'un admin.
- etc. ....

Systèmes affectés

- A priori **toutes** les distributions du socle uPortal et Esup-uPortal
- Correction faite en uportal-4.0.15 - uportal-4.0.15-esup-1 pour le packaging ESUP

Description

Un utilisateur capable de s'authentifier sur le CAS de l'établissement peut s'identifier sur l'ENT sous un autre login simplement via la construction et l'invocation d'une url (comportant notamment le login ciblé).

L'alerte concerne au moins les uPortal en 3.x et 4.x antérieurs au 21 Août 2014 (antérieurs à 4.0.15 / 4.1.1), et certainement les versions 2.x et inférieures également.

Elle concerne les uPortal utilisant l'authentification CAS avec une configuration classique de celle-ci : cela concerne donc la majorité des ENT EsupPortail de notre communauté.

Solution

Modifiez votre fichier security.properties (cf la description détaillée du workaround par Jasig) :

En lieu et place de

```
principalToken.root=userName
credentialToken.root=password
```

mettre

```
principalToken.root=
credentialToken.root=
principalToken.root.simple=userName
credentialToken.root.simple=password
```

Solution détaillée pour les différentes versions de esup-uPortal

esup-uPortal 4.x

La version uportal-4.0.15-esup-1 pour le package Esup corrige le problème. Si vous gérez votre ENT via Git, vous devriez ainsi pouvoir faire une mise à jour assez rapidement (git pull ou git merge puis redéploiement et redémarrage).

Le correctif dans le code ferme la vulnératibilité pour CAS, nous vous conseillons fortement aussi de modifier le fichier uportal-war/src/main/resources /properties/security.properties .

```
--- a/uportal-war/src/main/resources/properties/security.properties
+++ b/uportal-war/src/main/resources/properties/security.properties
@@ -40,8 +40,10 @@ root.simple=org.jasig.portal.security.provider.SimpleSecurityContextFactory

 ## Answers what tokens are examined in the request for each context during authentication.
 ## A subcontext only needs to set its tokens if it differs from those of the root context.
-principalToken.root=userName
-credentialToken.root=password
+principalToken.root=
+credentialToken.root=
+principalToken.root.simple=userName
+credentialToken.root.simple=password
 credentialToken.root.cas=ticket

 ## Answers where the user will be redirected when log out occurs. Each security context can have one.
```

esup-uPortal 3.2.x

Le fichier à modifier est update/uPortal/uportal-impl/src/main/resources/properties/security.properties ou custom/uPortal/uportal-impl/src/main/resources /properties/security.properties :

```
--- update/uPortal/uportal-impl/src/main/resources/properties/security.properties
+++ update/uPortal/uportal-impl/src/main/resources/properties/security.properties
@@ -42,8 +42,10 @@ root.remote=org.jasig.portal.security.provider.RemoteUserSecurityContextFactory

 ## Answers what tokens are examined in the request for each context during authentication.
 ## A subcontext only needs to set its tokens if it differs from those of the root context.
-principalToken.root=userName
-credentialToken.root=password
+principalToken.root=
+credentialToken.root=
+principalToken.root.simple=userName
+credentialToken.root.simple=password
 @esup.db.auth.comment@credentialToken.root.cas=ticket

 ## Answers where the user will be redirected when log out occurs. Each security context can have one.
```

Il faut ensuite faire

```
ant init deploy
```

Puis redémarrer tomcat.

esup-uPortal 2.6.x

Le fichier à modifier est update/uPortal/properties/security.properties ou custom/uPortal/properties/security.properties :

```
--- update/uPortal/properties/security.properties~      2009-12-10 14:59:10.000000000 +0100
+++ update/uPortal/properties/security.properties       2014-08-26 15:23:03.798027998 +0200
@@ -53,8 +53,10 @@

 # Answers what tokens are examined in the request for each context during authentication.
 # A subcontext only needs to set it's tokens if it differs from those of the root context.
-principalToken.root=userName
-credentialToken.root=password
+principalToken.root=
+credentialToken.root=
+principalToken.root.simple=userName
+credentialToken.root.simple=password

 # Answers where the user will be redirected when log out occurs. Each security context can have one.
 # (See comments in the LogoutServlet class)
```

Il faut ensuite faire

```
ant init deploy
```

Puis redémarrer tomcat.

Liens

- Issue Jasig https://issues.jasig.org/browse/UP-4192
- Description détaillée du workaround (modification de security.properties) : http://apetro.ghost.io/uportal-cve-2014-5059-workaround/
- Annonce de la faille sur Jasig et correctifs : http://jasig.275507.n4.nabble.com/CVE-2014-5059-CASified-uPortal-security-patch-td4663716.html