ESUP-2014-AVI-003 - Vulnérabilité dans les clients CAS

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 rediffuser 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 les clients CAS
Référence	ESUP-2014-AVI-003
Date de la première version	26 août 2014
Date de la dernière version	28 août 2014
Source	liste de diffusion uportal-user du consortium JASIG
Diffusion de cette version	Publique
Historique	• 11 août 2014 : réception de la faille CVE-2014-4172 sur cas-user • 26 août 2014 : prise en compte de la faille (Mathilde Guérin, Pascal Rigaux, Vincent Bonamy) • 26 août 2014 : rédaction de la première version de cet avis (Vincent Bonamy, Pascal Rigaux) • 26-28 août 2014 : reproduction de l'exploit sur les applications utilisant le client CAS JASIG (Vincent Bonamy, Pascal Rigaux) • 04 sept 2014 : envoi de l'avis de sécurité à securite@esup-portail.org • 02 oct 2014 : envoi de l'avis de sécurité à esup-utilisateurs@esup-portail.org
Planning prévisionnel	-
Pièces jointes	-

Risque

- Usurpation d'identité sur un service cassifié.

Systèmes affectés

- Applications cassifiées avec des librairies clientes CAS ne prenant pas en compte ce type d'attaque.
- Selon CVE-2014-4172 :

  Affected Software

  Jasig Java CAS Client
  Vulnerable versions: <3.3.2
  Fix version: 3.3.2, http://search.maven.org/#browse%7C1586013685

  .NET CAS Client
  Vulnerable versions: <1.0.2
  Fix version: 1.0.2,
  http://downloads.jasig.org/cas-clients/dotnet/dotnet-client-1.0.2-bin.zip

  phpCAS
  Vulnerable versions: <1.3.3
  Fix version: 1.3.3,
  http://downloads.jasig.org/cas-clients/php/1.3.3/CAS-1.3.3.tgz

- Concerne donc l'ENT EsupPortail, version < uportal-4.0.15 - uportal-4.0.15-esup-1 pour le packaging ESUP

Description

Une application extérieure (mise en place par le pirate) utilise le CAS de l'établissement comme mécanisme d'authentification (fonctionne si le CAS n'utilise pas de règles de filtrages "whitelist" sur les applications web cassifiées).
Un utilisateur va sur cette application (simple clic sur un lien par exemple) et fournit (après authentification CAS, qui se fait de manière transparente si une session CAS est déjà existante) de fait un service ticket à cette application. Le pirate utilise ce service ticket pour s'authentifier (au nom de l'utilisateur) sur l'ENT ou toute autre application cassifiée vulnérable, et ce alors que le ticket était à destination de l'application du pirate : exploitation de la faille.

Solutions

La mise en place des listes blanches des applications cassifiés sur le CAS de l'établissement a déjà été **fortement conseillée** dans l'alerte ESUP-2011-AVI-A. -

La mise à jour des librairies clientes CAS est une bonne option également, suite au signalement de cette faille les dernières versions corrigent ce problème.

Les applications web cassifiées impactées peuvent aussi proposer des mises à jour corrigeant ce problème.

- La mise à jour EsupPortail sur le tag uportal-4.0.15 permet de corriger le problème pour l'ENT EsupPortail par exemple
- Autre exemple, si vous utilisez CAS comme "authentication provider" pour votre IDP shibboleth, une mise à jour de la bibliothèque cas-client-core-xxx.jar peut être faite simplement pour sécuriser votre IDP vis à vis de cette faille.
- Plus généralement sur les applications Java utilisant la librairie cliente CAS Jasig, la mise à jour d'un cas-client-core-3.x.y.jar en cas-client-core-3.3.3.jar fixe le pb, de même que le passage sur spring-security 3.2.5.RELEASE (qui embarque cas-client-core-3.3.3.jar).

Solution détaillée pour esup-uPortal 3.x

Il faut modifier 2 fichiers pom.xml :

- si vous n'avez pas de fichier custom/uPortal/pom.xml, créez le :

```
cp update/uPortal/pom.xml custom/uPortal/pom.xml
```

- puis faites la modification :

```
--- custom/uPortal/pom.xml.old
+++ custom/uPortal/pom.xml
@@ -101,7 +101,7 @@
         <ant.version>1.7.1</ant.version>
         <aspectjrt.version>1.6.9</aspectjrt.version>
         <aspectjweaver.version>1.6.9</aspectjweaver.version>
-        <casclient.version>3.1.10</casclient.version>
+        <casclient.version>3.3.3</casclient.version>
         <cernunnos.version>1.2.1</cernunnos.version>
         <commons-cli.version>1.2</commons-cli.version>
         <commons-codec.version>1.4</commons-codec.version>
@@ -517,9 +517,15 @@
                 <version>${resource-aggregator.version}</version>
             </dependency>
             <dependency>
-                <groupId>org.jasig.cas</groupId>
+                <groupId>org.jasig.cas.client</groupId>
                 <artifactId>cas-client-core</artifactId>
                 <version>${casclient.version}</version>
+               <exclusions>
+                 <exclusion>
+                   <groupId>org.opensaml</groupId>
+                   <artifactId>opensaml</artifactId>
+                 </exclusion>
+               </exclusions>
             </dependency>
             <dependency>
                 <groupId>org.jasig.portal</groupId>
```

- si vous n'avez pas de fichier custom/uPortal/pom.xml ni update/uPortal/pom.xml, créez le :

```
cp Portail/uPortal*/uportal-impl/pom.xml custom/uPortal/uportal-impl/pom.xml
```

- puis faites la modification :

```
--- custom/uPortal/uportal-impl/pom.xml.old
+++ custom/uPortal/uportal-impl/pom.xml
@@ -96,11 +96,6 @@
                        <artifactId>esup-utils</artifactId>
                        <version>1.03</version>
                </dependency>
-               <dependency>
-                       <groupId>org.jasig.cas</groupId>
-                       <artifactId>cas-client-core</artifactId>
-                       <version>3.1.3</version>
-               </dependency>

         <!-- ***** Portal JDBC Driver *****
          | The groupId, artifactId and version are configured in the root POM.
@@ -118,7 +113,7 @@
         </dependency>

         <dependency>
-            <groupId>org.jasig.cas</groupId>
+            <groupId>org.jasig.cas.client</groupId>
             <artifactId>cas-client-core</artifactId>
         </dependency>
```

Liens

- Alerte mail sur cas-user : https://lists.wisc.edu/read/messages?id=33836937
- https://github.com/Jasig/cas-server-security-filter
- https://wiki.jasig.org/display/CAS/Frequently+Asked+Questions#FrequentlyAskedQuestions-Q:WhyshouldIusetheServicesManagementTool?ItseemslikeEFFORTtosetupanddeploy.