ESUP-2014-AVI-004 - Vulnérabilité dans esup-uPortal (3.2.4)

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 esup-uPortal-3.2.4
Référence	ESUP-2014-AVI-004
Date de la première version	2 oct 2014
Date de la dernière version	2 oct 2014
Source	liste de diffusion uportal-user du consortium JASIG
Diffusion de cette version	Publique
Historique	• 2 oct 2014 : prise en compte de la faille • 2 oct 2014 : rédaction de la première version de cet avis (Vincent Bonamy, Pascal Rigaux) • 7 oct 2014 : envoi de l'avis de sécurité à securite@esup-portail.org et esup-utilisateurs@esup-portail.org
Planning prévisionnel	-
Pièces jointes	-

Risque

- Usurpation d'identité sur un ENT Esup cassifié.

Systèmes affectés

- Cela concerne notamment la dernière version en 3.x d'Esup-uPortal, cette version est proposée ici : https://sourcesup.renater.fr/frs/?group_id=173
- Concerne donc a priori les ENT ESUP V3.2 en production à l'heure actuelle.
- Plus exhaustivement, les versions affectées sont celles qui ont été impactées par ce commit et qui n'ont pas reçu de corrections.

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 récupérer un TGT puis un Proxy Ticket pour s'authentifier (au nom de l'utilisateur) sur l'ENT : 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-2014-AVI-003 - Vulnérabilité dans les clients CAS""" - elle permet à nouveau ici d'inhiber fortement cette faille.

Cette faille très spécifique résulte cependant simplement de l'ajout impromptu du paramètre **acceptAnyProxy** à true dans le filtre CAS du socle uPortal lui même défini dans le fichier web.xml. La solution est donc de simplement supprimer cette propriété acceptAnyProxy (qui prend alors la valeur par défaut donnée false).

Solution détaillée pour esup-uPortal 3.2.4

Il faut modifier le fichier web.xml en supprimant le bloc suivant :

```
<init-param>
        <param-name>acceptAnyProxy</param-name>
        <param-value>true</param-value>
</init-param>
```

Liens

- Alerte mail sur uportal-user : http://jasig.275507.n4.nabble.com/uPortal-Security-Release-Notice-td4660097.html
- Issue Jasig : https://issues.jasig.org/browse/UP-3754
- Commit source du pb (avec versions affectées) : https://github.com/Jasig/uPortal/commit/af70a09cef5c875b2801c1953f99ba25dca1176f