ESUP-2014-AVI-001 - Vulnérabilité dans uPortal V4

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 uPortal V4
Référence	ESUP-2014-AVI-001
Date de la première version	24 mai 2014
Date de la dernière version	27 mai 2014
Source	liste de diffusion uportal-user du consortium JASIG
Diffusion de cette version	Publique
Historique	• 23 mai 2014 : réception de la faille • 23 mai 2014 : validation de la faille - vulnérabilité #1 (Vincent Bonamy) • 23 mai 2014 : mise en ligne d'un correctif pour le packaging EsupV4 (Vincent Bonamy) • 23 mai 2014 : envoi de l'avis de sécurité à securite@esup-portail.org • 27 mai 2014 : envoi de l'avis de sécurité à esup-utilisateurs@esup-portail.org
Planning prévisionnel	-
Pièces jointes	-

Risque

- Modification du contenu des pages des ENT (simple accès anonyme)
- Récupération d'informations personnelles (utilisateurs connectés)
- ....

Systèmes affectés

- Toutes les distributions 4.x du socle uPortal et Esup-uPortal
- correction faite en uportal-4.0.13.1 - uportal-4.0.13.1-esup-1 pour le packaging ESUP

Description

L'alerte concerne en fait 2 vulnérabilités. La première impacte effectivement les ENT V4 Esup en production. La deuxième ne devrait vraisemblablement impacter aucun ENT.

On propose ici une description simplifiée (vulgarisée - comporte donc des "raccourcis" ~ imprécisions) du descriptif donné par Jasig.
https://lists.wisc.edu/read/messages?id=33298597

Vulnérabilité #1

Un utilisateur pouvant afficher une portlet a la possibilité d'utiliser le mode "config" de la portlet (**en forgeant simplement l'url pour**).

Le mode "config" présente un formulaire qui permet de reconfigurer une portlet.

Très peu de portlets proposent ce mode config. Nous en identifions actuellement 2 :

- **Simplecontentportlet** : le mode config de cette portlet permet de modifier le contenu de la page via un éditeur wysiwyg. Il est très utilisé dans les ENT V4 notamment pour proposer des portlets présentant du contenu simple statique. De fait, on retrouve ces portlets dans les pages d'accueil des ENT pour l'accès public.
  Dans ces cas d'usage, la vulnérabilité #1 permet par exemple à tout internaute de modifier le contenu statique des pages publiques de l'ENT.

- **WebProxyPortlet** : le mode config de cette portlet permet de reparamétrer cette portlet. Cette portlet permet de faire proxy sur d'autres pages web.
  pour un usage public, la portlet peut être utilisé pour simplement afficher (faire 'proxy') une page externe - la vulnérabilité permet ainsi comme précédemment de modifier le contenu des pages de l'ENT par tout anonyme

pour un usage restreint, la portlet peut être utilisé comme mécanisme pour sécuriser certains accès - récupérer des pages web via une authentification "trusted"; cette vulnérabilité peut alors être exploitée par un utilisateur authentifié pour récupérer des informations qui étaient dédiées à un autre utilisateur.
Par exemple pour l'intégration de Moodle via une Webproxyportlet, cela peut permettre à un utilisateur de visualiser le listing des cours d'un autre utilisateur.

Vulnérabilité #2

Les utilisateurs pouvant administrer certaines portlets par délégation d'administration peuvent administrer toutes les portlets.

Dans les faits, il n'y a certainement aucun ENT qui utilise cette possibilité de délégation d'administration encore actuellement.

Solution

La version uportal-4.0.13.1 et uportal-4.0.13.1-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).

Vous pouvez aussi patcher uniquement les fichiers java uPortal en cause.

Pour la vulnérabilité #1 ceci est décrit ici :
https://gist.github.com/apetro/e56984a85f23d492c9c0#patch-application

et pour la vulnérabilité #2 - concerne pas (ou très peu) d'ENT :
https://gist.github.com/apetro/e49ece2ebc8ef0bdb31f#3-apply-the-fix-from-uportal-4014-as-a-patch-to-your-local-environment

Liens

- Annonce Publique Jasig des vulnérabilités et corrections : https://lists.wisc.edu/read/messages?id=33298597