Avis de sécurité 2007-001

Objet	Vulnérabilité dans *uPortal*
Référence	ESUP-2007-AVI-001
Date de la première version	20 août 2007
Date de la dernière version	3 septembre 2007
Source	Interne
Diffusion de cette version	Publique
Historique	20 août 2007 : découverte de la vulnérabilité (Julien MARCHAL) 21 août 2007 : mise au point du correctif (Vincent MATHIEU) 22 août 2007 : diffusion du correctif aux correspondants sécurité du consortium ESUP-Portail 3 septembre 2007 : annonce publique de la vulnérabilité
Pièces jointes	Aucune

Risque

Usurpation de l'identité des utilisateurs dans *uPortal* par récupération de l'identifiant de session.

Cet avis concerne uniquement les utilisateurs du canal *CWebProxy*.

Systèmes affectés

- Toutes les distributions *uPortal*
- Toutes les distributions *uPortal-esup*

Résumé

La configuration par défaut des canaux de type *CWebProxy* autorise une attaque de type *Cross Site Scripting* (*XSS*).

Utilisation et diffusion de ce document

Pour plus de renseignements : ***contact-tech@esup-portail.org***

Description

Par défaut, aucune restriction sur l'URI n'est spécifiée à la publication d'un canal de type *CWebProxy*.

La construction d'une URL falsifiant le paramètre **`cw_xml`** permet l'appel par le portail d'une page web quelconque. Cette page web, rendue par le portail, apparaît à l'utilisateur comme « de confiance » (puisque s'exécutant dans le portail) et peut notamment contenir du code *Javascript* dangereux.

Solution

Aucune mise à jour n'est nécessaire ; tout canal de type *CWebProxy* doit être configuré avec restriction sur les *URIs* appelables par le canal.

Cette configuration peut se faire :

1. De manière interactive, dans le portail sous un compte administrateur ;
2. Lors de la publication du canal à l'aide d'un fichier *XML*.

De manière interactive, dans le portail sous un compte administrateur

Depuis le canal « *channel manager* », choisir le canal en question, puis l'onglet « *URI restriction parameters* ». Le paramètre permettant de n'autoriser qu'une ou plusieurs *URIs* est « *Allowed URI prefixes* », la syntaxe est décrite dans la page.

Lors de la publication du canal à l'aide d'un fichier XML

Il suffit d'ajouter un paramètre supplémentaire nommé **`cw_allow_uri_prefixes`** :

```
<parameter>
  <name>cw_allow_uri_prefixes</name>
  <value>http://localhost/static/ http://univ.fr/ent/</value>
  <description></description>
  <ovrd></ovrd>
</parameter>
```

Seules les *URIs* commençant par les préfixes ainsi spécifiés seront autorisés.

Référence

http://www.mun.ca/portal/software/cw/