ESUP-2008-AVI-001 - 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 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
Référence	ESUP-2008-AVI-001
Date de la première version	18 juin 2008
Date de la dernière version	4 juillet 2008
Source	liste de diffusion uportal-user du consortium JASIG
Diffusion de cette version	Publique
Historique	• 17 juin 2008 : réception de la vulnérabilité • 18 juin 2008 : diffusion de l'avis de sécurité aux correspondants sécurité du consortium ESUP-Portail (Pascal Aubry) • 30 juin 2008 : diffusion publique de la vulnérabilité (Pascal Aubry) • 4 juillet 2008 : ajout d'un commentaire pour uPortal 2.5 (Julien Marchal)
Pièces jointes	ESUP-2008-AVI-001-COR.zip

Risque

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

Systèmes affectés

- Toutes les distributions uPortal depuis la version 3.0, 2.6 et avant
- Toutes les distributions uPortal-esup (basées sur uPortal 2.5 et 2.6)

Résumé

uPortal est distribué avec une configuration proxy qui autorise une attaque de type Cross Site Scripting (XSS).

Description

Un pirate peut introduire du code Javascript arbitraire dans le rendu de uPortal s'il fait ouvrir par le navigateur client une URL du portail malicieusement construite. Les possibilités d'attaque par le code Javascript incluent notamment la capture de l'identifiant de session, autorisant alors l'usurpation de l'identité de l'utilisateur.

Solution

La non utilisation de la servlet **HttpProxyServlet** était déjà recommandée par l'avis de sécurité ESUP-2007-AVI-001 - Vulnérabilité dans uPortal. Les exploitants qui n'utilisent pas cette servlet doivent vérifier qu'elle est bien commentée dans les fichiers **/WEB-INF/web.xml** de leurs instances de production.

Si la servlet est utilisée, ou qu'elle pourrait être utilisée, et que vous utilisez une version 2.6 ou plus, il faut alors remplacer le fichier **source/org/jasig /portal/HttpProxyServlet.java** par la version fournie dans le correctif ESUP-2008-AVI-001-COR.zip, puis redémarrer Tomcat.

> ⚠ **Solution pour uPortal 2.5**
>
> Dans le cas d'une version 2.5, vous devez obligatoire commenter la servlet **HttpProxyServlet** dans **/WEB-INF/web.xml**

Liens

- Le ticket JIRA montrant la vulnérabilité : http://www.ja-sig.org/issues/browse/UP-2088
- La page du wiki JASIG décrivant la vulnérabilité et donnant les solutions : http://www.ja-sig.org/wiki/x/YhPP

uPortal HttpProxyServlet security vulnerability and patch

by Andrew Petro < apetro@unicon.net >
June 17th 2008

*uPortal adopters,As you've likely seen on the JASIG announcement email list, uPortal 3.0.1 is now released. This release includes many improvements and Eric Dalquist and others are to be heartily congratulated.It also includes a specific critical security fix for a vulnerability in HttpProxyServlet, which affects both uPortal 3.0.0 and uPortal 2.6.1 and earlier.A patch is now available to fix this vulnerability in uPortal 2.6.*http://www.ja-sig.org/wiki/x/YhPP
If you are running the HttpProxyServlet (i.e., it is declared in web.xml), it is important that you apply this patch to secure from the risk of illicit proxies and cross-site-scripting through the vulnerability.Thanks are especially due to Dustin Schultz, Eric Dalquist, and others for their efforts in identifying and resolving this vulnerability.A uPortal 2.6.1.1 release (2.6.1 with this patch pre-applied) will be available for download shortly.Best wishes,Andrew