ESUP-2007-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-2007-AVI-001
Date de la première version	25 juillet 2007
Date de la dernière version	3 septembre 2007
Source	liste de diffusion jasig-members du consortium JASIG
Diffusion de cette version	Publique
Historique	• 25 juillet 2007 : réception de la vulnérabilité • 27 juillet 2007 : validation de la vulnérabilité sur le package uPortal-esup par le consortium ESUP-Portail (Julien MARCHAL) • 31 juillet 2007 : accord de Bill Thomson pour repousser l'annonce publique de la vulnérabilité au 15 août (à la place du 8 août) • 3 août 2007 : test du patch proposé et retour (négatif, ne marche que pour uPortal 2.6) à Bill THOMSON (Vincent MATHIEU) • 6 août 2007 : diffusion de la vulnérabilité aux correspondants sécurité du consortium ESUP-Portail • 15 août 2007 : mise en ligne d'un nouveau correctif (Susan BRAMHALL) • 18 août 2007 : validation du nouveau correctif (Vincent MATHIEU) • 21 août 2007 : envoi du correctif aux correspondants sécurité du consortium ESUP-Portail • 3 septembre 2007 : annonce publique de la vulnérabilité simultanément par les consortiums ESUP-Portail et JASIG
Pièces jointes	ESUP-2007-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 2.1
- Toutes les distributions uPortal-esup

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

Installer les classes du correctif ESUP-2007-AVI-001-COR.zipdans les sources de uPortal.

1. Positionner la propriété org.jasig.portal.serialize.ProxyWriter.resource_proxy_enabled du fichier portal.properties à off.
2. Commenter ou supprimer la servlet HttpProxyServlet dans le fichier WEB-INF/web.xml
3. Redéployer uPortal
4. Redémarrer Tomcat

XSS Vulnerability Proxy Exploit

by William G. Thompson Jr. < wgthom@rutgers.edu >
July 25th 2007

Summary

uPortal ships with a proxy configuration that allows illicit cross-site scripting. The Adversary can introduce arbitrary JavaScript into a user's portal render cycle if he or she can get the end user's web browser (e.g. via a hyperlink or a redirect) to open a cleverly crafted portal URL. The kinds of things the Adversary could accomplish with this JavaScript include capture of the user's otherwise secure session cookie, thereby allowing session hijacking.

Affected versions

uPortal 2.1, 2.2, 2.3, 2.4, 2.5

Issue

HttpProxyServlet:
uPortal ships with a proxy servlet allowing it to proxy over SSL content that would otherwise be vended in the clear so that the annoying "Mixed content" browser advisory message can be avoided. While some (many?) uPortal deployments are not using this servlet for anything, its default configuration is to be nonetheless latently available and so available for exploit using a cleverly crafted URL. You can turn off the feature of proxying resources via the portal.properties property "org.jasig.portal.serialize.ProxyWriter.resource_proxy_enabled" but this will not turn off the vulnerability. When this feature is deliberately used, its use involves detecting URLs needing to be re-written via a SAX filter and re-writing them to point at the proxy servlet which then proxies the originally intended content.

CWebProxy:
The proxy channel is not as severe an exploit as the HttpProxyServlet as an administrator has control over what content (sites) are published and to whom. Nonetheless, there is still a risk as it does proxy content similarly to HttpProxyServlet.

Resolution

uPortal will remember the URLs that it has re-written to be proxied, re-writing them with a user-session-render-cycle-specific serial number parameter rather than the URL itself needing to be proxied. The mapping of identifiers to URLs to be proxied is shared with the proxy servlet, which proxies the content on browser callback with a valid serial number parameter. The consequence is that the servlet will only proxy URLs the portal re-wrote intending to be proxied, rather than arbitrary URLs. CWebProxy will be resolved in a similar manner.

Alternatively, an upgrade to version 2.6.x will resolve this.

Patching

Eclipse Patch

Apply the included patch-2.5.txt Eclipse patch file, ignoring 9 leading path segments, against the uPortal "source" directory.

Add org.jasig.portal.serialize.ProxyFilter.java and org.jasig.portal.serialize.ProxyResourceMap.java from the included source .jar (new files not present in the Eclipse patch). Rebuild and re-deploy your uPortal.

Source Replacement

Expand the included source .jar over top of your uPortal 2.5 source, replacing the uPortal 2.5 source code with the new updated versions in the .jar. Rebuild and re-deploy your uPortal.

Binary Replacement

Add the .class files inside the included .jar file to your uPortal/WEB-INF/classes, overwriting existing .class files where they also appear in this .jar.

Endorsed .jar

Drop the included proxy-fix-2.5.jar into your tomcat/common/endorsed directory, causing the enclosed classes to supercede their precursors in your uPortal /WEB-INF/classes directory.

XSS Vulnerability Proxy Exploit

by Andrew Petro < apetro@unicon.net>
August 1st 2007

uPortal community,

It has become apparent that there are some issues with the patch included with this private, off-list vulnerability notification. Myself, Unicon, and others are actively re-testing the patch and working with people who have contacted me about getting this patch to work for them and we are developing a more robust, more widely-applicable patch.

In the meantime, I RECOMMEND THAT YOU DO NOT APPLY THE PREVIOUSLY POSTED PATCH TO PRODUCTION UPORTAL INSTANCES until the issues that have been discovered in the patch are better understood. The issues are not further security vulnerabilities so much as resource proxy functionality that doesn't work under the patch.

You can expect an errata writeup documenting those issues and providing a new version of the patch, I expect within the next few days.

The best response to this vulnerability for uPortal sites not using the resource proxy servlet is to remove it from the portal entirely. You can accomplish this by deleting outright the resource proxy servlet.class file (and source if you build from source).

To avoid further thrash in this larger context, the next release of this patch will first be made available to volunteers particularly interested in testing it. Several people have already contacted me off-list to volunteer for this task.

If you would like to test the next release of this patch and especially if you have experience and expertise in using resource proxies with uPortal, please do email me directly apetro@unicon.net and I will include you among the earliest testers of the updated patch.