

## IBM WebSphere Portal 'Portlet Palette' Cross-Site Scripting vulnerability

CVE reference: CVE-2010-0704

Vulnerability discovered: November 16, 2009

Discovered by: Sjoerd Resink, Fox-IT BV (<https://www.fox-it.com>)

Reported to vendor: January 11, 2010

Fix available: February 19, 2010 (<http://www-01.ibm.com/support/docview.wss?uid=swg1PM05829>)

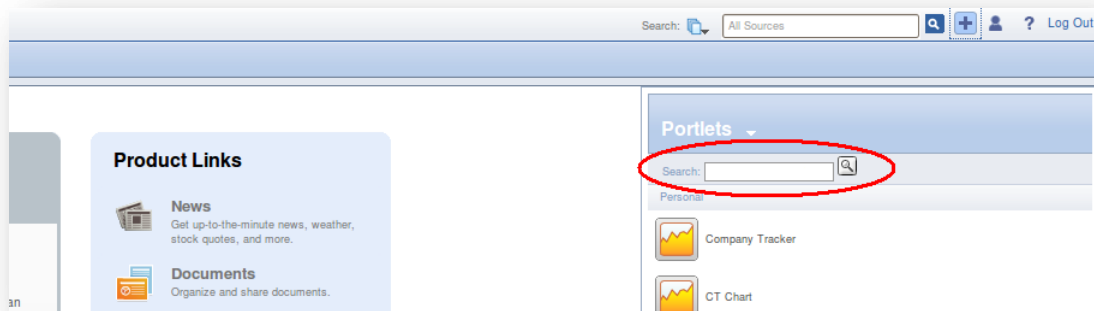
### Product

IBM® WebSphere® Portal consists of middleware applications (called portlets), and development tools for building and managing secure business-to-business (B2B), business-to-consumer (B2C), and business-to-employee (B2E) portals. More information can be found at:

[http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/topic/com.ibm.wp.ent.doc/wpf/intr\\_ovr.html](http://publib.boulder.ibm.com/infocenter/wpdoc/v6r0/topic/com.ibm.wp.ent.doc/wpf/intr_ovr.html)

### Vulnerability

The search field within the Portlet Palette of IBM WebSphere Portal is vulnerable to Cross-Site Scripting (XSS). The vulnerability specifically resides in the 'title' parameter. Authentication is required to exploit this vulnerability. Fox-IT verified that IBM WebSphere Portal version 6.0.1.5 Build Level wp6015\_008\_01 is vulnerable. It is unknown if other versions are affected as well.

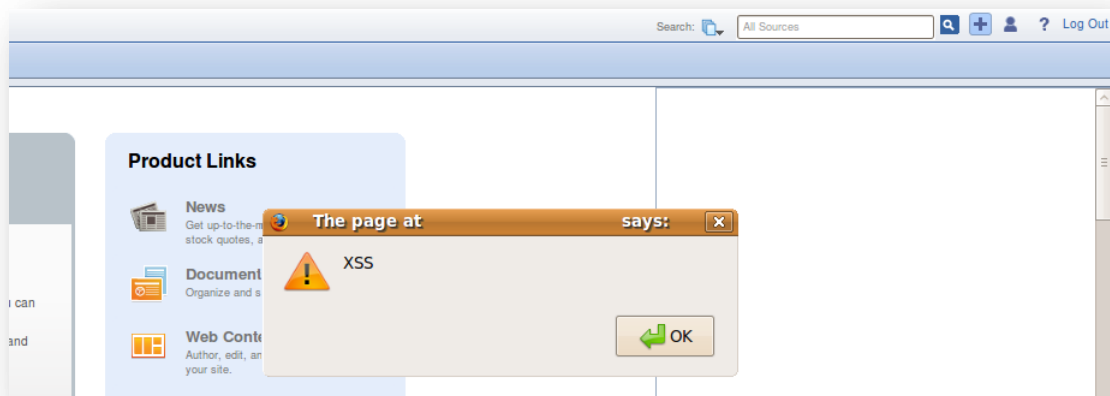


### Details

The XSS can be triggered by entering the following code in the search field of the Portlet Palette:

```
" style="position:absolute; top:-100px; left:-100px; width:10000px; height:10000px; z-index:999;" onmousemove="alert('XSS')">
```

Obviously, your mouse pointer must move over the field to trigger this XSS. The above code enlarges the search field.



Copyright © 2009 Fox-IT BV. All rights reserved.

Permission is granted for duplicating and distributing this advisory to the internet community for the purpose of information sharing and education, only if this advisory is not edited or altered in any way and is attributed to Fox-IT. Fox-IT is not liable for any misuse of this information by any third party.