
INetCop Security Advisory #2003-0x82-011

* Title: Buffer Overflow vulnerability in HTTP Fetcher Library.

0x01. Description

HTTP Fetcher is a small library that downloads files via HTTP.

More detailed personal information is

http://cs.nmu.edu/~lhanson/http_fetcher/README.

The library supports function as following.

http://cs.nmu.edu/~lhanson/http_fetcher/docs/

These mainly, is transplanted much to client.

Of course, is transplanted on server or many programs according to necessity.

If vulnerability exists in this library,

it may deal very fatal damage in transplanted program.

Yes, of course is so.

HTTP Fetcher library is exposed to very fatal buffer overflow.

And, It influences in other several programs.

Next time, functions are escaping buffer overflow only.

```
http_parseFilename();
```

```
http_setReferer();
```

```
http_setUserAgent();
```

```
example> t=malloc(strlen(x)); strcpy(t,x);
```

But, requestBuf devours together 'Referer buffer' and 'UserAgent buffer',
URL that user inputs etc.. in http_fetch() function.
So, because of requestBuf array, problem happens.

See http_fetch() function in 'http_fetcher.c' code.

http_fetch() function:

```
—  
 97             sprintf(requestBuf, "GET %s %s \n", charIndex, HTTP_VERSION);  
105             strcat(requestBuf, host); // Here, URL buffer overflow.  
111             strcat(requestBuf, referer); // Here, Referer buffer overflow.  
126             strcat(requestBuf, userAgent); // Here, UserAgent buffer overflow.  
--
```

They happen by strcat() function.

0x02. Vulnerable Packages

Vendor site: http://cs.nmu.edu/~lhanson/http_fetcher/

http fetcher 1.0.1

- http-fetcher-dev_1.0.1_i386.deb

- http-fetcher_1.0.1_i386.deb

- http_fetcher-1.0.1-1.i386.rpm

- http_fetcher-1.0.1-1.src.rpm

- **http_fetcher-1.0.1.tar.gz**

+Linux

+Other

http fetcher 1.0.0

- http_fetcher-1.0.0.tar.gz

0x03. Exploit

As this is different according to purpose that program is made out, can become exploit. There is very good target program of 'fetch'. He's playing client role. (<http://cs.nmu.edu/~lhanson/fetch/>)

Because used dangerous http_fetch library, 'fetch' program becomes exploit as following.

```
bash$ ./0x82-test.sucksfetch.xpl
target: "./fetch"
len: 1135
jmp addr: 0xbffffb98
netcat 0 31337.
Connected to 0.
id
uid=501(x82) gid=501(x82) groups=501(x82)
exit
bash$
```

Hehe, we did not find actuality program to do exploit yet.
'fetch' gives nothing to us.
It's test only.

0x04. Patch

```
=== http_fetcher.patch ===
```

```
--- http_fetcher.c      Tue Jul 31 03:47:15 2001
+++ http_fetcher.patch.c  Thu Jan  2 22:24:48 2003
@@ -94,7 +94,7 @@
         *      request */
         sprintf(requestBuf, "GET / %s \n", HTTP_VERSION);
     else
```

```
-         sprintf(requestBuf, "GET %s %s \n", charIndex, HTTP_VERSION);
+         snprintf(requestBuf, sizeof(requestBuf)/4-1, "GET %s %s \n", charIndex,
HTTP_VERSION);
```

```
/* Null out the end of the hostname if need be */
```

```
if(charIndex != NULL)
```

```
@@ -102,13 +102,13 @@
```

```
/* Use Host: even though 1.0 doesn't specify it. Some servers
```

```
* won't play nice if we don't send Host, and it shouldn't hurt anything */
```

```
strcat(requestBuf, "Host: ");
```

```
- strcat(requestBuf, host);
```

```
+ strncpy(requestBuf, host, sizeof(requestBuf)/4-1);
```

```
strcat(requestBuf, " \n");
```

```
if(!hideReferer && referer != NULL) /* NO default referer */
```

```
{
```

```
strcat(requestBuf, "Referer: ");
```

```
- strcat(requestBuf, referer);
```

```
+ strncpy(requestBuf, referer, sizeof(requestBuf)/4-1);
```

```
strcat(requestBuf, " \n");
```

```
}
```

```
@@ -123,7 +123,7 @@
```

```
else if(!hideUserAgent)
```

```
{
```

```
strcat(requestBuf, "User-Agent: ");
```

```
- strcat(requestBuf, userAgent);
```

```
+ strncpy(requestBuf, userAgent, sizeof(requestBuf)/4-1);
```

```
strcat(requestBuf, " \n");
```

```
}
```

```
=== 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>

--