

[UNIX] pServ Directory Traversal Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0020.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/05/04

To: list@securiteam.com

Date: 5 Jan 2004 16:51:51 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

pServ Directory Traversal Vulnerability

SUMMARY

The aim of <<http://sourceforge.net/projects/pserv>> pServ (pico Server) is "to create a portable, small web server. Coded in portable C with UNIX being the main reference platform, but porting is encouraged. Portability and small footprint should enable the use of pServ on a workstation as well as". A directory traversal vulnerability in the product allows remote attackers to view files that reside outside the bound HTTP root directory.

DETAILS

Vulnerable systems:

* pServ version 3.0b2

The program, by default, has an anti-directory traversal check, but this check can be easily bypassed using the double slash ("/") into the HTTP requests.

Exploit:

To test the pServ's vulnerability simply send to the web server an HTTP request string, like that:

```
GET ../../ HTTP/1.0\r\n\r\n
```

Securiteam: [UNIX] pServ Directory Traversal Vulnerability

Or generally:

```
GET ../../MY_PATH HTTP/1.0\r\n\r\n
GET /SOME_DIRECTORY//...// HTTP/1.0\r\n\r\n
```

Therefore, the web server will allow you to go outside of the documentsPath assigned to the web server, and navigate through the system.

Solution:

To fix the bug simply go on the pServ's official website, <http://sourceforge.net/projects/pserv> and download the latest version of pServ (see in CVS).

Or, if you want, you can use my following little patch, that should fix the bug for the version 3.0b2 of pServ:

```
--- main.c 2003-09-22 10:39:24.000000000 +0200
+++ patch.c 2003-12-19 12:40:47.000000000 +0100
@@ -455,6 +455,11 @@
     dirName[1] = req.documentAddress[2];
     dirName[2] = req.documentAddress[3];
     dirName[3] = '\0';
+ if (dirName[0] == '/')
+ {
+ sayError(sock, FORBIDDEN, req.documentAddress,
+ req);
+ return -1;
+ }
     if (!strcmp(dirName, ".."))
     {
         sayError(sock, FORBIDDEN, req.documentAddress,
+ req); @@ -462,6 +467,15 @@
     }
     }
     j = 0;
+ for(i = 1; i < sL; i++) {
+ if(req.documentAddress[i] == '/')
+ if(req.documentAddress[i+1] == '/')
+ {
+ sayError(sock, FORBIDDEN,
+ req.documentAddress, req);
+ return -1;
+ }
+ }
     for (i = 1; i < sL; i++) {
         if (req.documentAddress[i] == '/')
         {
```

ADDITIONAL INFORMATION

Securiteam: [UNIX] pServ Directory Traversal Vulnerability

The information has been provided by <mailto:fdonato@autistici.org>
Donato Ferrante.

=====

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.