
INetCop Security Advisory #2002-0x82-005

* Title: Remote POST Buffer Overflow vulnerability in Pserv (Pico Server).

0x01. Description

Pico server is very small webserver of C language base that support several platforms.

Webserver has very interesting function that watch buffer overflow basically.

(Developer seems to hate very buffer overflow. ; -)

Can confirm as following.

```
—  
bash# cat *.c | grep flow  
    printf("Buffer overflow on document path parsing \n");  
    { /* checking for buffer overflow */  
        printf("Buffer overflow on POST read \n");  
        if (totalRead > BUFFER_SIZE) /* checking for buffer overflow */  
            printf("Buffer overflow on request read \n");
```

```
bash#
```

```
--
```

There's thing which among them, there is no substantiality.

Indicate wrong part in 184 line to main.c.

This part is POST method area.

```
—
178     reqSize = strlen(req);
179     i = 0; j = 0;
180     while (i < MAX_REQUEST_LINES && j < reqSize)
181     {
182         k = 0;
183         while (req[j] != '\n')
184             token[k++] = req[j++]; // here.
185         token[k-1] = '\0'; /* the line read ends with an \n we skipit and count it as
read */
186         j++;
187         strcpy(reqArray[i], token);
188         i++;
189     }
--
```

Through POST method, can attempt Denial of Service (DoS) Attack.

0x02. Vulnerable Packages

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

Pserv 2.0 beta 3

-pserv-31-Oct-02.tar.Z

+MacOS X

+AIX

+NetBSD

+Linux

2.0 beta 2

-pserv-20-Oct-02.tar.Z

2.0 beta 1

-pserv-15-Oct-02.tar.Z

2.0 alpha 12

-pserv-18-Sep-02.tar.Z

2.0 alpha 11

-pserv-17-Sep-02.tar.Z

2.0 alpha 10

-pserv-10-Sep-02.tar.Z

2.0 alpha 9

-pserv-09-Sep-02.tar.Z

2.0 alpha 8

-pserv-04-Sept-02.tar.Z

2.0 alpha 7

-pserv-29-Aug-02.tar.Z

2.0 alpha 6

-pserv-24-Aug-02.tar.Z

2.0 alpha 5

-pserv-22-Aug-02.tar.Z

2.0 alpha 4

-pserv-17-Aug-02.tar.Z

2.0 alpha 3

-pserv-11-Aug-02.tar.Z

2.0 alpha 2

-pserv-10-Aug02.tar.Z

2.0 alpha 1

-pserv-7-Aug-02.tar

1.0

-pserv1.0.tgz

* I did not other version exploit test. but, It may be weak.

0x03. Exploit

Do you want exploit code? Very regrettable. :- (

We don't want to compose DoS code.

0x04. Patch

=== http.patch ===

```
- - - main.c      Tue Nov 19 16:48:40 2002
+++ main.patch.c  Tue Nov 19 16:15:51 2002
@@ -176,6 +176,9 @@
```

```
    /* we copy the header lines to an array for easier parsing */
```

```
    reqSize = strlen(req);
```

```
+
```

```
+   req[BUFFER_SIZE]='\ n'; /* Limit! */
```

```
+
```

```
    i = 0; j = 0;
```

```
    while (i < MAX_REQUEST_LINES && j < reqSize)
```

```
    {
```

```
=== 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>

--