

[NEWS] myServer Vulnerable to Terminated Connection DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0031.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/15/03

To: list@securiteam.com

Date: 15 Jun 2003 21:50:21 +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

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>,
or call 617-399-6980

myServer Vulnerable to Terminated Connection DoS

SUMMARY

<<http://myserverweb.sourceforge.net>> myServer Web is a "free and easy to configure web server". The product has been found to contain a vulnerability that allows remote attackers to cause the product to crash by disconnecting right after a connection is established.

DETAILS

Vulnerable systems:

* myServer version 0.4.1

Example:

```
# telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^'.
```

Securiteam: [NEWS] myServer Vulnerable to Terminated Connection DoS

```

[Ctrl]+C
Connection closed by foreign host.
# gdb -c core
GNU gdb 5.0mdk-11mdk Linux-Mandrake 8.0
Copyright 2001 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and
you are
welcome to change it and/or distribute copies of it under certain
conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for
details.
This GDB was configured as "i386-mandrake-linux".
Core was generated by `./myserver'.
Program terminated with signal 11, Segmentation fault.
#0 0x40187f92 in ?? ()
(gdb) bt
#0 0x40187f92 in ?? ()
#1 0x08053bc0 in ?? ()
#2 0x0804e744 in ?? ()
#3 0x40093817 in ?? ()

```

Vendor response:

The same problem was reported on the WIN32 platform. The error was found in the HTTP protocol parser that work correctly only when find a valid http header. This bug, that can be cause of DoS attacks will be absent in the imminent next release of MyServer, actually wasn't tested on Linux but it will be. Thanks for your note.

ADDITIONAL INFORMATION

The information has been provided by <mailto:_LynX[at]bk.ru> LynX.

=====

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.