

[NEWS] Thompson (Alcatel) SpeedTouch Home ADSL Modem Predictable TCP ISN Generation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0023.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/09/04

To: list@securiteam.com

Date: 9 Aug 2004 19:36:07 +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>

Thompson (Alcatel) SpeedTouch Home ADSL Modem Predictable TCP ISN Generation

SUMMARY

The Thompson (formerly Alcatel) <http://www.speedtouchdsl.com/>

SpeedTouch is an ADSL router for home and business providing a continuously available, "always on," connection.

Remote exploitation of a design error vulnerability in Thompson's SpeedTouch Home ADSL modem allows attackers to spoof TCP traffic on behalf of the device.

DETAILS

Vulnerable Systems:

* Thompson's SpeedTouch firmware version GV8BAA3.270 (1003825), possibly prior

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0641>

CAN-2004-0641

Securiteam: [NEWS] Thompson (Alcatel) SpeedTouch Home ADSL Modem Predictable TCP ISN Generation

The problem specifically exists due to the predictable nature of the TCP Initial Sequence Number (ISN) generator on the device. The following sanitized tcpdump output demonstrates the existence of the vulnerability when 10 consecutive TCP connection requests are generated for the telnet server (port 23) on the Thompson device:

```
48.3 host_a.1096 > host_b.telnet: S
48.3 host_b.telnet > host_a.1096: S 4081040897:4081040897(0) ack
48.3 host_a.1096 > host_b.telnet: R
48.4 host_a.1096 > host_b.telnet: S
48.4 host_b.telnet > host_a.1096: S 4081104897:4081104897(0) ack
48.4 host_a.1096 > host_b.telnet: R
48.6 host_a.1096 > host_b.telnet: S
48.6 host_b.telnet > host_a.1096: S 4081232897:4081232897(0) ack
48.6 host_a.1096 > host_b.telnet: R
48.7 host_a.1096 > host_b.telnet: S
48.7 host_b.telnet > host_a.1096: S 4081296897:4081296897(0) ack
48.7 host_a.1096 > host_b.telnet: R
48.9 host_a.1096 > host_b.telnet: S
48.9 host_b.telnet > host_a.1096: S 4081360897:4081360897(0) ack
48.9 host_a.1096 > host_b.telnet: R
49.0 host_a.1096 > host_b.telnet: S
49.0 host_b.telnet > host_a.1096: S 4081488897:4081488897(0) ack
49.0 host_a.1096 > host_b.telnet: R
49.2 host_a.1096 > host_b.telnet: S
49.2 host_b.telnet > host_a.1096: S 4081552897:4081552897(0) ack
49.2 host_a.1096 > host_b.telnet: R
49.3 host_a.1096 > host_b.telnet: S
49.3 host_b.telnet > host_a.1096: S 4081616897:4081616897(0) ack
49.3 host_a.1096 > host_b.telnet: R
49.5 host_a.1096 > host_b.telnet: S
49.5 host_b.telnet > host_a.1096: S 4081744897:4081744897(0) ack
49.5 host_a.1096 > host_b.telnet: R
49.6 host_a.1096 > host_b.telnet: S
49.6 host_b.telnet > host_a.1096: S 4081808897:4081808897(0) ack
49.6 host_a.1096 > host_b.telnet: R
```

In the above example, host_a is the querying host and host_b is the Thompson device. A clear pattern in ISN generation can be seen as the value increases by approximately 64,000 each millisecond.

Successful exploitation of weak ISNs for the purpose of connection spoofing is not a trivial task. Successful exploitation allows an attacker to generate traffic on behalf of the affected device.

Disclosure Timeline

- 06/08/04 Initial vendor contact – no response
- 06/08/04 iDEFENSE clients notified
- 06/18/04 Secondary vendor contact – no response
- 08/05/04 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by
<mailto:idlabs-advisories@idefense.com> iDEFENSE Security Labs.

=====

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.