

# [Full-disclosure] DNS and Checkpoint

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-07/msg00109.html>

---

- *From:* imipak <[imipak@xxxxxxxxx](mailto:imipak@xxxxxxxxx)>
  - *Date:* Wed, 9 Jul 2008 15:00:39 +0100
- 

Hello everyone,

I've had a report from someone with clue (and tcpdump) that a properly functioning DNS resolver that correctly uses randomised source ports magically becomes vulnerable once the traffic's passed through a Checkpoint firewall, where Dan Kaminsky's tool shows:

```
x.y.z.155:56978 TXID=712
x.y.z.155:56979 TXID=45713
x.y.z.155:56980 TXID=63532
x.y.z.155:56981 TXID=7243
x.y.z.155:56982 TXID=17620
```

(note the incrementing port numbers.)

Can anyone else confirm this behaviour?

Checkpoint are one of the dozens of vendors listed on the CERT advisory as "Status: Unknown"

<http://www.kb.cert.org/vuls/id/MIMG-7ECL6B>

They do have an advisory up:

<http://www.checkpoint.com/defense/advisories/public/2008/cpai-01-Jul.html>

I don't have the login needed to read the whole thing, but the front page just says:

```
"Protection provided by:
VPN-1: * NGX R65
* NGX R62
* NGX R61
* NGX R60
[...etc, etc...] "
```

cheers

=i

## [Full-disclosure] DNS and Checkpoint

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>