

FreeBSD-Security: use keep state(strict) to mitigate tcp issues?

use keep state(strict) to mitigate tcp issues?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-04/0172.html>

From: Mipam (*mipam_at_ibt.net*)

Date: 04/23/04

Date: Fri, 23 Apr 2004 15:17:32 +0200 (MET DST)

To: <freebsd-security@freebsd.org>

Hi,

When deploying a BSD with IPF in at the network perimeter and using rules like these:

```
pass in .. proto tcp ... keep state(strict)
```

it's possible to refuse tcp packets which arrive out of order. This would increase the difficulty doing blind attack resets and blind data injection attack, cause then you'd have to "guess" the exact expected number. Checkpoint has a similar feature (is that right?) which is described here as the answer to the mentioned attacks:

http://www.checkpoint.com/techsupport/alerts/tcp_dos.html

Although this is nice, there is also the risk of breaking connection because it's not unlikely that packets arrive out of order.

At least, that's what i think, any thoughts upon this?

Bye,

Mipam.

freebsd-security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"