

Re: sacrificing performance for confusion

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/performance/2003-06/0110.html>

From: Jeff Roberson (jroberson_at_chesapeake.net)

Date: 06/27/03

Date: Thu, 26 Jun 2003 21:04:24 -0400 (EDT)

To: "D. J. Bernstein" <djb@cr.yp.to>

On 26 Jun 2003, D. J. Bernstein wrote:

> > *Using VMM protection to forbid code execution within the DATA, BSS, heap,*
> > *and stack (if one can) mitigates against a common class of problems--*
>
> *I don't believe you. Show me a real program that's (1) vulnerable if*
> *data/bss/heap/stack are executable and (2) invulnerable otherwise.*
>
> *Yes, attacks are often written to take advantage of executable stacks;*
> *but, in every case I've investigated, the programs would still have been*
> *vulnerable with non-executable stacks.*

They would be vulnerable to a denial of service but not to any privilege gaining exploit.

Please go spread FUD somewhere else. We're not going to put all of your sections in the same page. Nobody cares.

Cheers,
Jeff

freebsd-performance@freebsd.org mailing list

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

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