

Re: Non-Executable Stack Patch

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-06/0037.html>

From: David Schultz (das_at_FreeBSD.ORG)

Date: 06/08/03

Date: Sat, 7 Jun 2003 17:59:27 -0700
To: Erik Paulsen Skaalerud <erik@pentadon.com>

On Thu, Jun 05, 2003, Erik Paulsen Skaalerud wrote:

> > *From:* owner-freebsd-security@freebsd.org
> > [<mailto:owner-freebsd-security@freebsd.org>] *On Behalf Of* Tim Baur
> > *Sent:* Thursday, June 05, 2003 6:24 AM
> > *To:* freebsd-security@freebsd.org
> > *On Wed, 4 Jun 2003, Tony Meman wrote:*
> > > *I was wondering if there's any non-executable stack patch for*
> > > *FreeBSD's kernel.*
> > <http://www.trl.ibm.com/projects/security/ssp/buildfreebsd.html>
> >
> > *-tbaur*
>
> *Can anyone here share their experiences with this patch? I've heard very*
> *little talk about it really, I'm looking for others oppinions before I try*
> *to patch gcc with this. Any major slowdowns on the userland? And if its*
> *major, how much?*

The original StackGuard implementation had massive overhead: several orders of magnitude for common programs. It looks like the fellows at IBM have managed to do significantly better:

<http://www.trl.ibm.com/projects/security/ssp/node5.html>

I personally am not particularly interested in a fix that makes buffer overflows harder to exploit, given that buffer overflows constitute a problem that can be completely solved without the same performance loss by switching to a safer language. Nevertheless, there's enough useful C code out there that this could be useful. It would be cool to have as an optional part of FreeBSD, assuming we wouldn't have to maintain massive diffs against gcc or something. (gcc uses this by default now, right?)

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"