

RE: realpath(3) et al

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-08/0133.html>

From: Devon H. O'Dell (dodell_at_sitetronics.com)

Date: 08/12/03

To: <security@freebsd.org>

Date: Tue, 12 Aug 2003 13:24:50 +0200

Sorry for not including this in the last message to the newsletter; isn't it also then high time to fix up the signal handling in FreeBSD if this *is* the case?

Kind regards,

Devon H. O'Dell
Systems and Network Engineer
Simpli, Inc. Web Hosting
<http://www.simpli.biz>

> -----Oorspronkelijk bericht-----

> Van: owner-freebsd-security@freebsd.org [mailto:owner-freebsd-

> security@freebsd.org] Namens Devon H. O'Dell

> Verzonden: Tuesday, August 12, 2003 1:21 PM

> Aan: 'Peter Jeremy'

> CC: security@freebsd.org

> Onderwerp: RE: realpath(3) et al

>

> It, would though, be trivial to implement this with a #define based upon
> the

> kernel configuration, would it not? Protecting against stack smashing is

> quite important; I think many hosting environments not using LISP or other

> executable-stack-reliant packages would benefit from this. By negating the

> ability to execute injected code through a buffer overflow, security is

> highly increased. By implementing it as a kernel configuration option, I

> don't think we would lose out at all.

>

> Kind regards,

>

> Devon H. O'Dell

> Systems and Network Engineer

> Simpli, Inc. Web Hosting

> <http://www.simpli.biz>

>

>> -----Oorspronkelijk bericht-----

>> Van: owner-freebsd-security@freebsd.org [mailto:owner-freebsd-

FreeBSD-Security: RE: realpath(3) et al

> > *security@freebsd.org*] Namens Peter Jeremy
> > *Verzonden: Tuesday, August 12, 2003 1:15 PM*
> > *Aan: Devon H. O'Dell*
> > *CC: security@freebsd.org*
> > *Onderwerp: Re: realpath(3) et al*
> >
> > *On Tue, Aug 12, 2003 at 11:02:16AM +0200, Devon H. O'Dell wrote:*
> > > *Features such as a protected stack should, IMO, be implemented as soon*
> > *as*
> > > *possible to keep FreeBSD heads-afloat right now in the security*
> > *sense....*
> > > *OpenBSD has implemented this already and there are many patches for*
> > *Linux*
> > *to*
> > > *do the same... why don't we go ahead and shove some of this code into*
> > *CVS?*
> >
> > *By "protected" I presume you mean "non-executable". Whilst making the*
> > *stack non-executable is trivial, making the system still work isn't.*
> > *I believe the FreeBSD signal handling still relies on a signal*
> > *trampoline on the stack. Some ports also expect an executable stack*
> > *(most commonly lisp implementations).*
> >
> > *Some years ago, I tried implementing a non-executable stack on a*
> > *Solaris box. Interleaf promptly stopped working so I had to undo the*
> > *change.*
> >
> > *Peter*
> >
> > _____
> > *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"*
> >
> >
> > _____
> > *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"*

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"