Subject: Re: [PATCH] IA64,sparc: local DoS with corrupted ELFs
Posted by Willy Tarreau on Fri, 08 Sep 2006 04:34:12 GMT
View Forum Message <> Reply to Message

On Thu, Sep 07, 2006 at 04:42:07PM -0700, Andrew Morton wrote:
> On Thu, 7 Sep 2006 22:07:14 +0200
> Willy Tarreau <w@1wt.eu> wrote:
>
> > On Thu, Sep 07, 2006 at 08:17:04AM -0700, Linus Torvalds wrote:
> > >
> > >
> > > On Thu, 7 Sep 2006, Kirill Korotaev wrote:
> > > >
> > > > Does the patch below looks better?
> > >
> > > Yes.
> > >
> > > Apart from the whitespace corruption, that is.
> > >
> > > I don't know how to get mozilla to not screw up whitespace.
>
> Me either. I've had a bug report in the mozilla system for maybe four
> years concerning space-stuffing. Occasionally it comes to life but afaict
> nothing ever changes.
>
> I expect it'd be pretty easy to undo the space-stuffing in git.

Perhaps, but it should not be up to the versionning system to decide to
change the contents of the patches which get merged. Otherwise, we will
not be able to trust it as much as today.

> In extremis I just do s/^ /^ / and it works. An automated solution would
> need to recognise the appropriate headers (Format=Flowed, iirc).

perhaps for this case, but then what will prevent us from trying to
implement dirtier features such as line un-wrapping ?

> > maybe by using it to download mutt or something saner ? :-)
> >
> > More seriously, while we don't like email attachments because they make
> > it impossible to comment on a patch, maybe we should encourage people
> > with broken mailers to post small patches in both forms :
> >   - pure text for human review (spaces are not much of a problem here)
> >   - MIME to apply the patch.
>
> argh. That means that email contains two copies of the patch. So it
> applies with `patch --dry-run' then causes havoc with `patch'

except if the text version is mangled in order not to be detected as
a patch. I suspect that inserting a space in front of "---" is enough
for patch not to find it. Don't get me wrong, I know this is dirty.
But as long as some people will use broken mailers, we'll get broken
patches. Some people occasionnaly switch to attachments stating they
have broken mailers, and others even post links to their patches,
which is annoying for potential reviewers. If we could give them
strict rules on how to proceed when they have such problems, it would
make the job easier for others.

willy