[perl #130635] [PATCH] Stack overflow in Storable retrieve_hook

Thread Previous

From:
Tony Cook via RT

Date:
January 30, 2017 05:12
Subject:
[perl #130635] [PATCH] Stack overflow in Storable retrieve_hook
Message ID:
rt-4.0.24-382-1485753120-1608.130635-15-0@perl.org

```
On Sat, 28 Jan 2017 16:41:50 -0800, john@nixnuts.net wrote:
> On Thu, 2017-01-26 at 13:48 -0800, James E Keenan via RT wrote:
> > As previously reported, I configure with:
> >
> > "-des -Dusedevel -Duseithreads -Doptimize='-O2 -pipe -fstack-
> > protector -fno-
> > strict-aliasing' -DDEBUGGING"
> >
> > ... because that gets us very close to the way that the FreeBSD port
> > of perl
> > is configured.
> >
>
> Excellent, thanks.
>
> The problem turned out to be that the AFL generated payload was
> hitting two
> other memory allocation errors before it even entered retrieve_hook().
> That
> combination of flags on FreeBSD seems to crash whenever Storable tries
> to
> allocate too much memory.
>
> I adjusted the test data to use more realistic sizes when it enters
> retrieve_hash() and retrieve_flag_hash() so that it's only focusing on
> the stack
> overflow in retrieve_hook().
>
> I also cleaned up the test output formatting a bit.
>
> An updated patch is attached.

Won't the allocated buffer leak if the load_module() fails, no STORABLE_thaw is defined, or if STORABLE_thaw dies?

Tony


---
via perlbug:  queue: perl5 status: open
https://rt.perl.org/Ticket/Display.html?id=130635
```

Thread Previous

- Re: [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by John Lightsey
- [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by Tony Cook via RT
- Re: [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by John Lightsey
- Re: [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by John Lightsey
- [perl #130635] [PATCH] Stack overflow in Storable retrieve_hook by James E Keenan via RT
- **[perl #130635] [PATCH] Stack overflow in Storable retrieve_hook** by Tony Cook via RT