

Perl / perl5 Public[Code](#) [Issues](#) 2.2k [Pull requests](#) 157 [Actions](#) [Projects](#) [Wiki](#) [Security](#)[New issue](#)

[PATCH] Stack overflow in Storable retrieve_hook #15831

✓ ClosedLabels distro-All hasPatch type-library

p5pRT opened on Jan 24, 2017

Migrated from [rt.perl.org#130635](https://rt.perl.org/#130635) (status was 'resolved')

Searchable as RT130635\$



p5pRT on Jan 24, 2017

Author

From @lightsey

Created by @lightsey

This is a bug report for perl from john@nixnuts.net,
generated with the help of perlbug 1.40 running under perl 5.25.9.

AFL detected a stack overflow in Storable's retrieve_hook() function.

The problem essentially is that a hook's classname length is read into a signed integer, compared to the size of a stack buffer, then used to read the classname. The size comparison treats the length as signed, while the read treats the length as unsigned.

[▶ Perl Info](#)

p5pRT on Jan 24, 2017

Author

From @lightsey

► 0001-Fix-stack-buffer-overflow-in-deserialization-of-hook.patch



p5pRT on Jan 25, 2017

Author

**From @jkeenan**

On Tue, 24 Jan 2017 19:22:28 GMT, john@nixnuts.net wrote:

This is a bug report for perl from john@nixnuts.net,
generated with the help of perlbug 1.40 running under perl 5.25.9.

AFL detected a stack overflow in Storable's retrieve_hook() function.

The problem essentially is that a hook's classname length is read into a signed integer, compared to the size of a stack buffer, then used to read the classname. The size comparison treats the length as signed, while the read treats the length as unsigned.

Available for smoke-testing in this branch:

smoke-me/jkeenan/130635-storable

I corrected one spelling error in a test description and incremented the VERSION number.

--

James E Keenan (jkeenan@cpan.org)



p5pRT on Jan 25, 2017

Author



The RT System itself - Status changed from 'new' to 'open'



p5pRT on Jan 25, 2017

Author

**From @jkeenan**

On Wed, 25 Jan 2017 02:05:45 GMT, jkeenan wrote:

On Tue, 24 Jan 2017 19:22:28 GMT, john@nixnuts.net wrote:

This is a bug report for perl from john@nixnuts.net,
generated with the help of perlbug 1.40 running under perl 5.25.9.

AFL detected a stack overflow in Storable's retrieve_hook() function.

The problem essentially is that a hook's classname length is read into a signed integer, compared to the size of a stack buffer, then used to read the classname. The size comparison treats the length as signed, while the read treats the length as unsigned.

Available for smoke-testing in this branch:

smoke-me/jkeenan/130635-storable

I corrected one spelling error in a test description and incremented the VERSION number.

This revision failed on FreeBSD-11. See: <http://perl5.test-smoke.org/report/53470>

When I ran the test file individually, it hung at 'ok 24', then printed these error messages:

```
#####
```

```
swap_pager: out of swap space  
swap_pager_getswapspace(16): failed  
swap_pager_getswapspace(16): failed  
swap_pager_getswapspace(16): failed
```

```
#####
```

```
kernel: pid 18627 (perl), uid 1001, was killed: out of swap space
```

So something is clearly amiss with this patch.

Thank you very much.

--

James E Keenan (jkeenan@cpan.org)



p5pRT on Jan 25, 2017

Author



From @jkeenan

On Wed, 25 Jan 2017 04:04:15 GMT, jkeenan wrote:

On Wed, 25 Jan 2017 02:05:45 GMT, jkeenan wrote:

On Tue, 24 Jan 2017 19:22:28 GMT, john@nixnuts.net wrote:

This is a bug report for perl from john@nixnuts.net,
generated with the help of perlbug 1.40 running under perl 5.25.9.

AFL detected a stack overflow in Storable's retrieve_hook()
function.

The problem essentially is that a hook's classname length is read
into
a signed integer, compared to the size of a stack buffer, then used
to
read the classname. The size comparison treats the length as
signed,
while the read treats the length as unsigned.

Available for smoke-testing in this branch:

smoke-me/jkeenan/130635-storable

I corrected one spelling error in a test description and incremented
the VERSION number.

This revision failed on FreeBSD-11. See: <http://perl5.test-smoke.org/report/53470>

When I ran the test file individually, it hung at 'ok 24', then
printed these error messages:

```
#####  
swap_pager: out of swap space  
swap_pager_getswapspace(16): failed  
swap_pager_getswapspace(16): failed  
swap_pager_getswapspace(16): failed  
#####
```

kernel: pid 18627 (perl), uid 1001, was killed: out of swap space

So something is clearly amiss with this patch.

Thank you very much.

Similar results on FreeBSD-10.3:

<http://perl5.test-smoke.org/report/53481>

--

James E Keenan (jkeen@cpan.org)



p5pRT on Jan 25, 2017

Author ...

From @jkeenan

On Wed, 25 Jan 2017 15:21:36 GMT, jkeenan wrote:

On Wed, 25 Jan 2017 04:04:15 GMT, jkeenan wrote:

On Wed, 25 Jan 2017 02:05:45 GMT, jkeenan wrote:

On Tue, 24 Jan 2017 19:22:28 GMT, john@nixnuts.net wrote:

This is a bug report for perl from john@nixnuts.net,
generated with the help of perlbug 1.40 running under perl 5.25.9.

AFL detected a stack overflow in Storable's retrieve_hook()
function.

The problem essentially is that a hook's classname length is read
into
a signed integer, compared to the size of a stack buffer, then used
to
read the classname. The size comparison treats the length as
signed,
while the read treats the length as unsigned.

Available for smoke-testing in this branch:

smoke-me/jkeenan/130635-storable

I corrected one spelling error in a test description and incremented
the VERSION number.

This revision failed on FreeBSD-11. See: <http://perl5.test-smoke.org/report/53470>

When I ran the test file individually, it hung at 'ok 24', then
printed these error messages:

```
#####  
swap_pager: out of swap space  
swap_pager_getswapspace(16): failed  
swap_pager_getswapspace(16): failed  
swap_pager_getswapspace(16): failed  
#####
```

kernel: pid 18627 (perl), uid 1001, was killed: out of swap space

So something is clearly amiss with this patch.

Thank you very much.

Similar results on FreeBSD-10.3:

<http://perl5.test-smoke.org/report/53481>

On (at least) FreeBSD-10.3, it appears that the test failure occurs when I configure with -DDEBUGGING:

```
#####
```

```
[perl] $ gitcurr
```

```
130635-storable
```

```
[perl] $ git show | head -1
```

```
commit 706cfb1
```

```
[perl] $ ./perl -llib -V | grep config_args
```

```
config_args='-des -Dusedevel -Duseithreads -Doptimize=-O2 -pipe -fstack-protector -fno-strict-aliasing -DDEBUGGING'
```

```
#####
```

```
cd t;./perl harness -v ../dist/Storable/t/store.t; cd -
```

```
...
```

```
ok 24 - RT 130098: no segfault in Storable::fd_retrieve()
```

```
# Failed test 'No stack smashing error when retrieving hook'
```

```
# at t/store.t line 109.
```

```
# Looks like you failed 1 test of 25.
```

```
not ok 25 - No stack smashing error when retrieving hook
```

```
Dubious, test returned 1 (wstat 256, 0x100)
```

```
Failed 1/25 subtests
```

```
...
```

```
#####
```

In the same branch, at the same commit, configuring exactly the same except without -DDEBUGGING, the test file completes successfully.

```
--
```

James E Keenan (jkeenan@cpan.org)



p5pRT on Jan 25, 2017

Author



From @lightsey

On Wed, 2017-01-25 at 07:21 -0800, James E Keenan via RT wrote:

On Wed, 25 Jan 2017 04:04:15 GMT, jkeenan wrote:

This revision failed on FreeBSD-11. See: <http://perl5.test-smoke.org/report/53470>

^

When I ran the test file individually, it hung at 'ok 24', then printed these error messages:

^

```
#####
```

```
swap_pager: out of swap space
swap_pager_getswapspace(16): failed
swap_pager_getswapspace(16): failed
swap_pager_getswapspace(16): failed
```

```
#####
```

^

```
kernel: pid 18627 (perl), uid 1001, was killed: out of swap space
```

^

So something is clearly amiss with this patch.

^

Thank you very much.

Similar results on FreeBSD-10.3:

<http://perl5.test-smoke.org/report/53481>

Makes sense.. When the bug is fixed, it ends up allocating an insanely large amount of memory. On Linux, malloc doesn't even try to allocate the memory. It sounds like BSD does try to allocate it.

Maybe it's possible to limit the maximum allowed classname length to what Perl actually supports. I'll try and adjust the patch to do this.



p5pRT on Jan 25, 2017

Author



From @jkeenan

On Wed, 25 Jan 2017 15:42:21 GMT, jkeenan wrote:

On Wed, 25 Jan 2017 15:21:36 GMT, jkeenan wrote:

On Wed, 25 Jan 2017 04:04:15 GMT, jkeenan wrote:

On Wed, 25 Jan 2017 02:05:45 GMT, jkeenan wrote:

On Tue, 24 Jan 2017 19:22:28 GMT, john@nixnuts.net wrote:

```
This is a bug report for perl from john@nixnuts.net,
generated with the help of perlbug 1.40 running under perl
5.25.9.
```

AFL detected a stack overflow in Storable's retrieve_hook() function.

The problem essentially is that a hook's classname length is read into a signed integer, compared to the size of a stack buffer, then used to read the classname. The size comparison treats the length as signed, while the read treats the length as unsigned.

Available for smoke-testing in this branch:

smoke-me/jkeenane/130635-storable

I corrected one spelling error in a test description and incremented the VERSION number.

This revision failed on FreeBSD-11. See: <http://perl5.test-smoke.org/report/53470>

When I ran the test file individually, it hung at 'ok 24', then printed these error messages:

```
#####
```

```
swap_pager: out of swap space  
swap_pager_getswapspace(16): failed  
swap_pager_getswapspace(16): failed  
swap_pager_getswapspace(16): failed
```

```
#####
```

```
kernel: pid 18627 (perl), uid 1001, was killed: out of swap space
```

So something is clearly amiss with this patch.

Thank you very much.

Similar results on FreeBSD-10.3:

<http://perl5.test-smoke.org/report/53481>

On (at least) FreeBSD-10.3, it appears that the test failure occurs when I configure with -DDEBUGGING:

```
#####
[perl] $ gitcurr
130635-storable
[perl] $ git show | head -1
commit 706cfb1
[perl] $ ./perl -llib -V | grep config_args
config_args='-des -Dusedevel -Duseithreads -Doptimize=-O2 -pipe
-fstack-protector -fno-strict-aliasing -DDEBUGGING'
#####
cd t;./perl harness -v ../dist/Storable/t/store.t; cd -
...
ok 24 - RT 130098: no segfault in Storable::fd_retrieve()

# Failed test 'No stack smashing error when retrieving hook'
# at t/store.t line 109.
# Looks like you failed 1 test of 25.
not ok 25 - No stack smashing error when retrieving hook
Dubious, test returned 1 (wstat 256, 0x100)
Failed 1/25 subtests
...
#####
```

In the same branch, at the same commit, configuring exactly the same except without `-DDEBUGGING`, the test file completes successfully.

On FreeBSD-11, I get the same difference in results between with/without `-DDEBUGGING`.

On Linux, with `-DDEBUGGING`, the test file eventually completes ... but clearly hangs for some time after 'ok 21' and takes 30s to run.

So the patch does not play well with `-DDEBUGGING` regardless of OS.

Thank you very much.

--

James E Keenan (jkeenan@cpan.org)



p5pRT on Jan 25, 2017

Author



From @lightsey

On Wed, 2017-01-25 at 08:12 -0800, James E Keenan via RT wrote:

On FreeBSD-11, I get the same difference in results between with/without `-DDEBUGGING`.

On Linux, with `-DDEBUGGING`, the test file eventually completes ... but clearly hangs for some time after 'ok 21' and takes 30s to run.

So the patch does not play well with -DDEBUGGING regardless of OS.

Thank you very much.

I'm attaching an updated patch that croaks before these oversized New() calls rather than trying to handle the failures they generate.



p5pRT on Jan 25, 2017

Author ...

From @lightsey

▶ 0001-Fix-stack-buffer-overflow-in-deserialization-of-hook.patch



p5pRT on Jan 25, 2017

Author ...

From @jkeenan

On Wed, 25 Jan 2017 19:44:02 GMT, john@nixnuts.net wrote:

On Wed, 2017-01-25 at 08:12 -0800, James E Keenan via RT wrote:

On FreeBSD-11, I get the same difference in results between with/without -DDEBUGGING.

On Linux, with -DDEBUGGING, the test file eventually completes ... but clearly hangs for some time after 'ok 21' and takes 30s to run.

So the patch does not play well with -DDEBUGGING regardless of OS.

Thank you very much.

I'm attaching an updated patch that croaks before these oversized New() calls rather than trying to handle the failures they generate.

On Linux, with a -DDEBUGGING build, the runtime of the test came down to a reasonable length.

However on both FreeBSD 10 and 11, the results under `-DDEBUGGING` were still unsatisfactory. Running the test manually on 10.3, I had to Ctrl-C the test after 2 minutes. Running smoke tests on 11, it appears that the test completed successfully once but then got the same swap errors previously reported, leading to the curious result of "PASS-so-far":

<http://perl5.test-smoke.org/report/53487>

--

James E Keenan (jkeenan@cpan.org)



p5pRT on Jan 26, 2017

Author



From @lightsey

On Wed, 2017-01-25 at 14:31 -0800, James E Keenan via RT wrote:

On Wed, 25 Jan 2017 19:44:02 GMT, john@nixnuts.net wrote:

On Wed, 2017-01-25 at 08:12 -0800, James E Keenan via RT wrote:

On FreeBSD-11, I get the same difference in results between with/without `-DDEBUGGING`.

On Linux, with `-DDEBUGGING`, the test file eventually completes ... but clearly hangs for some time after 'ok 21' and takes 30s to run.

So the patch does not play well with `-DDEBUGGING` regardless of OS.

Thank you very much.

Â

I'm attaching an updated patch that croaks before these oversized `New()` calls rather than trying to handle the failures they generate.

On Linux, with a `-DDEBUGGING` build, the runtime of the test came down to a reasonable length.

However on both FreeBSD 10 and 11, the results under `-DDEBUGGING` were still unsatisfactory.Â Â Running the test manually on 10.3, I had to Ctrl-C the test after 2 minutes.Â Â Running smoke tests on 11, it appears that the test completed successfully once but then got the same swap errors previously reported, leading to the curious result of "PASS-so-far":

<http://perl5.test-smoke.org/report/53487>

I brought up a FreeBSD 10.3 AMD64 VM to test and saw a similar issue when I ran the new unit test with the older version of Storable. The long pause on BSD seemed to be caused by coredumps being enabled (default on FreeBSD, not default on Linux.)

I didn't see any crashes on the FreeBSD VM when testing bleed with the new version of the patch. The configure settings I used were:

```
./Configure -des -DDEBUGGING -Dusedevel
```

Is it possible that some of the failures you're seeing were caused by using the wrong version of Storable?



p5pRT on Jan 26, 2017

Author



From @jkeenan

On Thu, 26 Jan 2017 21:02:12 GMT, john@nixnuts.net wrote:

On Wed, 2017-01-25 at 14:31 -0800, James E Keenan via RT wrote:

On Wed, 25 Jan 2017 19:44:02 GMT, john@nixnuts.net wrote:

On Wed, 2017-01-25 at 08:12 -0800, James E Keenan via RT wrote:

On FreeBSD-11, I get the same difference in results between with/without -DDEBUGGING.

On Linux, with -DDEBUGGING, the test file eventually completes ... but clearly hangs for some time after 'ok 21' and takes 30s to run.

So the patch does not play well with -DDEBUGGING regardless of OS.

Thank you very much.

I'm attaching an updated patch that croaks before these oversized New() calls rather than trying to handle the failures they generate.

On Linux, with a -DDEBUGGING build, the runtime of the test came down to a reasonable length.

However on both FreeBSD 10 and 11, the results under `-DDEBUGGING` were still unsatisfactory. Running the test manually on 10.3, I had to Ctrl-C the test after 2 minutes. Running smoke tests on 11, it appears that the test completed successfully once but then got the same swap errors previously reported, leading to the curious result of "PASS-so-far": <http://perl5.test-smoke.org/report/53487>

I brought up a FreeBSD 10.3 AMD64 VM to test and saw a similar issue when I ran the new unit test with the older version of Storable. The long pause on BSD seemed to be caused by coredumps being enabled (default on FreeBSD, not default on Linux.)

I didn't see any crashes on the FreeBSD VM when testing bleed with the new version of the patch. The configure settings I used were:

```
./Configure -des -DDEBUGGING -Dusedevel
```

Is it possible that some of the failures you're seeing were caused by using the wrong version of Storable?

I used the most recent version of this branch in the perl 5 repository:

```
smoke-me/jkeenan/130635-storable
```

... which I believe incorporates your revised patch.

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.

Thank you very much.

--

James E Keenan (jkeenan@cpan.org)



p5pRT on Jan 29, 2017

Author ...

From @lightsey

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.

17 remaining items

Load more

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Metadata**Assignees**

No one assigned

Labels

distro-All

hasPatch

type-library

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants

