openQA Project - action #104164

The openSUSE package perl-App-cpanminus was suggested for removal but we rely on it within openQA size:M

2021-12-19 20:44 - okurz

Status:	Resolved	**Start date:**	2021-12-19
Priority:	High	**Due date:**	2022-02-11
Assignee:	osukup	**% Done:**	0%
Category:	Organisational	**Estimated time:**	0.00 hour
Target version:	Ready		
Difficulty:			

Description

Motivation

https://build.opensuse.org/request/show/940824 suggests to remove the package
https://build.opensuse.org/package/show/openSUSE:Factory/perl-App-cpanminus with reasoning

> Unsafe and no release since 2018
> https://blog.hackeriet.no/cpan-signature-verification-vulnerabilities/

We use that e.g. in https://github.com/os-autoinst/openQA/search?q=cpanm in container/openqa/entrypoint.sh, tools/run-tests-within-container, dist/rpm/openQA.spec, etc. Also in os-autoinst scope https://github.com/search?q=org%3Aos-autoinst+perl-App-cpanminus.*&type=code , e.g. in https://github.com/os-autoinst/os-autoinst/blob/b4cc32462b7dc6ae196455325b8a4495d18bc62c/tools/container_run_ci and https://github.com/os-autoinst/os-autoinst-distri-openQA/blob/53747261a2e74bd4788b23e0b101a95ca962eabf/tests/install/openqa_webui.pm so we should look to assess the situation, find mitigations or suggest a way to have a fixed version of perl-App-cpanminus. As I see sufficient activity in https://github.com/miyagawa/cpanminus/commits/devel maybe we should switch the package to checkout from that branch instead of CPAN releases.

Acceptance criteria

- **AC1:** openQA is not vulnerable to any of the mentioned CVEs
- **AC2:** The package perl-App-cpanminus has not been removed from Factory (or we are using an alternative like curl -L https://cpanmin.us | perl - -M https://cpan.metacpan.org ...)

History

#1 - 2021-12-20 07:38 - osukup

probably the best approach will be port patches from cpanminus repository to current package.

+- I found two relevant commits in repo

and then with new release update to new stable

#2 - 2021-12-20 09:38 - osukup

- Assignee set to osukup

#3 - 2021-12-20 15:07 - kraih

I don't think we ever even used Module::Signature with cpanm. You're getting worked up about nothing.

#4 - 2021-12-20 15:12 - kraih

But there are security best practices we should enforce, such as the use of a trusted mirror, and strict HTTPS connections. I don't think we do either at the moment.

#5 - 2021-12-20 15:16 - kraih

The most trusted and generally very fast (CDN backed) mirror is https://cpan.metacpan.org. It's what the Mojolicious installation one-liners use (curl -L https://cpanmin.us | perl - -M https://cpan.metacpan.org -n Mojolicious). If the package was not in openSUSE anymore we could switch to curl. But of course installing via zypper would be slightly better for security.

#6 - 2021-12-20 15:26 - kraih

I'll start by making a PR that fixes all current uses of cpanm to use the bare minimum security best practices. (Not assigning the ticket to me, but assume i'm on it...)

#7 - 2021-12-20 15:39 - kraih

Opened a PR. https://github.com/os-autoinst/openQA/pull/4421

#8 - 2021-12-20 16:35 - kraih

And merged. That means all our uses of cpanm are now through a trusted HTTPS mirror and reasonably secure.

#9 - 2021-12-21 10:54 - tinita

I asked miyagawa here when a release is planned: https://github.com/miyagawa/cpanminus/pull/636#issuecomment-998678526

#10 - 2021-12-21 14:08 - osukup

Upstream stopped releasing cpanminus on CPAN with version 1.7044 , git has tagged 1.9017 and devel version reports 1.9020

So I repacked perl-App-cpanminus with devel version - sr: https://build.opensuse.org/request/show/941820

#11 - 2021-12-21 17:20 - tinita

I tried out the package from https://build.opensuse.org/request/show/941820

There are some differences to the current rpm package. Some cpanminus files are missing, and Menlo files are additional. not sure if this is how it should work:

```
% rpm -ql perl-App-cpanminus
                           [p5.26.3] 17:50:25
/usr/bin/cpanm
/usr/lib/perl5/vendor_perl/5.26.1/App
/usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus
/usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus.pm
/usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus.pod
/usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus/Dependency.pm
/usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus/fatscript.pm
/usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus/script.pm
/usr/lib/perl5/vendor_perl/5.26.1/x86_64-linux-thread-multi
/usr/share/doc/packages/perl-App-cpanminus
/usr/share/doc/packages/perl-App-cpanminus/Changes
/usr/share/doc/packages/perl-App-cpanminus/README
/usr/share/licenses/perl-App-cpanminus
/usr/share/licenses/perl-App-cpanminus/LICENSE
/usr/share/man/man1/cpanm.1.gz
/usr/share/man/man3/App::cpanminus.3pm.gz
/usr/share/man/man3/App::cpanminus::fatscript.3pm.gz

% rpm -ql perl-App-cpanminus-1.9020-0.noarch.rpm
                           [p5.26.3] 17:50:27
/usr/bin/cpanm
/usr/lib/perl5/vendor_perl/5.34.0/App
/usr/lib/perl5/vendor_perl/5.34.0/App/cpanminus
/usr/lib/perl5/vendor_perl/5.34.0/App/cpanminus.pm
/usr/lib/perl5/vendor_perl/5.34.0/App/cpanminus/script.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo
/usr/lib/perl5/vendor_perl/5.34.0/Menlo.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Builder
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Builder/Static.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/CLI
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/CLI/Compat.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Dependency.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Index
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Index/MetaCPAN.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Index/MetaDB.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Index/Mirror.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Legacy.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Util.pm
/usr/share/doc/packages/perl-App-cpanminus
/usr/share/doc/packages/perl-App-cpanminus/Changes
/usr/share/doc/packages/perl-App-cpanminus/README.md
/usr/share/licenses/perl-App-cpanminus
/usr/share/licenses/perl-App-cpanminus/LICENSE
/usr/share/man/man1/cpanm.1.gz
```

```
/usr/share/man/man3/App::cpanminus.3pm.gz
/usr/share/man/man3/Menlo.3pm.gz
/usr/share/man/man3/Menlo::Builder::Static.3pm.gz
/usr/share/man/man3/Menlo::CLI::Compat.3pm.gz
/usr/share/man/man3/Menlo::Index::MetaCPAN.3pm.gz
/usr/share/man/man3/Menlo::Index::MetaDB.3pm.gz
/usr/share/man/man3/Menlo::Legacy.3pm.gz
```

We are still hoping that the author is replying to us about his release plans.

#12 - 2021-12-22 10:15 - kraih

Spoke with upstream, a new App::cpanminus should be released soon and the --verify functionality will probably be deprecated completely.

#13 - 2021-12-23 10:21 - kraih

- Description updated

#14 - 2021-12-28 08:30 - cdywan

- Status changed from New to In Progress

I give in. I'm updating the status now

#15 - 2021-12-29 04:11 - openqa_review

- Due date set to 2022-01-12

Setting due date based on mean cycle time of SUSE QE Tools

#16 - 2022-01-04 09:17 - osukup

tinita wrote:

> I tried out the package from https://build.opensuse.org/request/show/941820
>
> There are some differences to the current rpm package. Some cpanminus files are missing, and Menlo files are additional. not sure if this is how it should work:
>
> ```
> % rpm -ql perl-App-cpanminus
>                                [p5.26.3] 17:50:25
> /usr/bin/cpanm
> /usr/lib/perl5/vendor_perl/5.26.1/App
> /usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus
> /usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus.pm
> /usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus.pod
> /usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus/Dependency.pm
> /usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus/fatscript.pm
> /usr/lib/perl5/vendor_perl/5.26.1/App/cpanminus/script.pm
> /usr/lib/perl5/vendor_perl/5.26.1/x86_64-linux-thread-multi
> /usr/share/doc/packages/perl-App-cpanminus
> /usr/share/doc/packages/perl-App-cpanminus/Changes
> /usr/share/doc/packages/perl-App-cpanminus/README
> /usr/share/licenses/perl-App-cpanminus
> /usr/share/licenses/perl-App-cpanminus/LICENSE
> /usr/share/man/man1/cpanm.1.gz
> /usr/share/man/man3/App::cpanminus.3pm.gz
> /usr/share/man/man3/App::cpanminus::fatscript.3pm.gz
>
> % rpm -ql perl-App-cpanminus-1.9020-0.noarch.rpm
>                                [p5.26.3] 17:50:27
> /usr/bin/cpanm
> /usr/lib/perl5/vendor_perl/5.34.0/App
> /usr/lib/perl5/vendor_perl/5.34.0/App/cpanminus
> /usr/lib/perl5/vendor_perl/5.34.0/App/cpanminus.pm
> /usr/lib/perl5/vendor_perl/5.34.0/App/cpanminus/script.pm
> /usr/lib/perl5/vendor_perl/5.34.0/Menlo
> /usr/lib/perl5/vendor_perl/5.34.0/Menlo.pm
> /usr/lib/perl5/vendor_perl/5.34.0/Menlo/Builder
> /usr/lib/perl5/vendor_perl/5.34.0/Menlo/Builder/Static.pm
> /usr/lib/perl5/vendor_perl/5.34.0/Menlo/CLI
> /usr/lib/perl5/vendor_perl/5.34.0/Menlo/CLI/Compat.pm
> /usr/lib/perl5/vendor_perl/5.34.0/Menlo/Dependency.pm
> /usr/lib/perl5/vendor_perl/5.34.0/Menlo/Index
> ```

```
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Index/MetaCPAN.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Index/MetaDB.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Index/Mirror.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Legacy.pm
/usr/lib/perl5/vendor_perl/5.34.0/Menlo/Util.pm
/usr/share/doc/packages/perl-App-cpanminus
/usr/share/doc/packages/perl-App-cpanminus/Changes
/usr/share/doc/packages/perl-App-cpanminus/README.md
/usr/share/licenses/perl-App-cpanminus
/usr/share/licenses/perl-App-cpanminus/LICENSE
/usr/share/man/man1/cpanm.1.gz
/usr/share/man/man3/App::cpanminus.3pm.gz
/usr/share/man/man3/Menlo.3pm.gz
/usr/share/man/man3/Menlo::Builder::Static.3pm.gz
/usr/share/man/man3/Menlo::CLI::Compat.3pm.gz
/usr/share/man/man3/Menlo::Index::MetaCPAN.3pm.gz
/usr/share/man/man3/Menlo::Index::MetaDB.3pm.gz
/usr/share/man/man3/Menlo::Legacy.3pm.gz
```

> We are still hoping that the author is replying to us about his release plans.

current package is fatpack with everything in one file , on other hand new is normal perl package

#17 - 2022-01-17 17:04 - cdywan

- Due date changed from 2022-01-12 to 2022-01-21

Acceptance criteria

- **AC1:** openQA is not vulnerable to any of the mentioned CVEs
- **AC2:** The package perl-App-cpanminus has not been removed from Factory (or we are using an alternative like curl -L https://cpanmin.us | perl - -M https://cpan.metacpan.org ...)

osukup @sriedel So where are we at?

#18 - 2022-01-18 14:59 - osukup

cdywan wrote:

> ## Acceptance criteria
>
> - **AC1:** openQA is not vulnerable to any of the mentioned CVEs
> - **AC2:** The package perl-App-cpanminus has not been removed from Factory (or we are using an alternative like curl -L https://cpanmin.us | perl - -M https://cpan.metacpan.org ...)
>
> osukup @sriedel So where are we at?

AC1: my SR solves this
AC2:

1) delete request was rejected/postponed
2) my SR to Factoryt repapackage devel version of cpanm (as is used by upstream, which stopped publishing cpanm on CPAN)

#19 - 2022-01-18 15:00 - osukup

updated SR contains removal of checksum functions

#20 - 2022-01-19 08:31 - cdywan

osukup wrote:

> updated SR contains removal of checksum functions

https://build.opensuse.org/request/show/947240 This?

#21 - 2022-01-19 09:28 - osukup

cdywan wrote:

> osukup wrote:
>
> > updated SR contains removal of checksum functions
>
> https://build.opensuse.org/request/show/947240 This?

ja :D

#22 - 2022-01-25 11:58 - osukup

- Status changed from In Progress to Feedback

.. for next step it needs SR accepted and forwarded to Factory (Then submitted to Leap)

#23 - 2022-01-25 15:33 - tinita

See:

- https://github.com/miyagawa/cpanminus/pull/636
- https://github.com/miyagawa/cpanminus/issues/639
- https://github.com/miyagawa/cpanminus/pull/638

So Miyagawa says the feature will be removed (PR 638).
Unfortunately there is still no release, but we could try to backport the patch to the current tarball, it seems simple enough.
But I also asked him again what the plans are.

I vote against https://build.opensuse.org/request/show/947240 , and there were several comments from me and others on this and the previous request https://build.opensuse.org/request/show/941820

> current package is fatpack with everything in one file , on other hand new is normal perl package

That's not the only difference.

#24 - 2022-01-25 15:43 - kraih

tinita wrote:

> See:
>
> - https://github.com/miyagawa/cpanminus/pull/636
> - https://github.com/miyagawa/cpanminus/issues/639
> - https://github.com/miyagawa/cpanminus/pull/638
>
> So Miyagawa says the feature will be removed (PR 638).
> Unfortunately there is still no release, but we could try to backport the patch to the current tarball, it seems simple enough.
> But I also asked him again what the plans are.
>
> I vote against https://build.opensuse.org/request/show/947240 , and there were several comments from me and others on this and the previous request https://build.opensuse.org/request/show/941820

I'm with Tina on this.

#25 - 2022-01-27 11:09 - tinita

A new release was just made: https://metacpan.org/dist/App-cpanminus 1.7045

#26 - 2022-01-27 11:41 - osukup

- Status changed from Feedback to In Progress

with new release thanks to tinita --> on Friday 28.1 is excepted to be in devel project and created ticket to Factory

in middle of next week accepted into Factory and then we can create MR to Leap 15.3 with in +- 10 days released as Maint Update for leap

#27 - 2022-01-27 16:50 - osukup

- Status changed from In Progress to Feedback

#28 - 2022-01-27 17:57 - cdywan

osukup If we're waiting on something that'll happen in ~10 days I would think Feb 11 seems like a good due date, because by then we should be able to have this verified and resolved.

#29 - 2022-01-28 09:26 - tinita

- Due date changed from 2022-01-21 to 2022-02-11

Request for Factory: https://build.opensuse.org/request/show/949627

#30 - 2022-01-31 12:39 - osukup

SR to factory accepted

MR to Leap 15.3 https://build.opensuse.org/request/show/950151

#31 - 2022-02-02 11:28 - cdywan

osukup wrote:

> SR to factory accepted
>
> MR to Leap 15.3 https://build.opensuse.org/request/show/950151

I see a build issue unresolvable: nothing provides perl(aliased) for i586. Are you looking into it? Or is this expected?

#32 - 2022-02-07 09:39 - osukup

cdywan wrote:

> osukup wrote:
>
> > SR to factory accepted
> >
> > MR to Leap 15.3 https://build.opensuse.org/request/show/950151
>
> I see a build issue unresolvable: nothing provides perl(aliased) for i586. Are you looking into it? Or is this expected?
> i586 isnt supported :D

btw accepted as openSUSE:Maintenance:17366

#33 - 2022-02-10 11:26 - cdywan

- Subject changed from The openSUSE package perl-App-cpanminus was suggested for removal but we rely on it within openQA to The openSUSE package perl-App-cpanminus was suggested for removal but we rely on it within openQA size:M

- Status changed from Feedback to Resolved

Both ACs are fulfilled, the package no longer has the unwanted features and remains in factory