NAME

perl5303delta - what is new for perl v5.30.3

DESCRIPTION

This document describes differences between the 5.30.2 release and the 5.30.3 release.

If you are upgrading from an earlier release such as 5.30.1, first read perl5302delta, which describes differences between 5.30.1 and 5.30.2.

Security

[CVE-2020-10543] Buffer overflow caused by a crafted regular expression

A signed "size_t" integer overflow in the storage space calculations for nested regular expression quantifiers could cause a heap buffer overflow in Perl's regular expression compiler that overwrites memory allocated after the regular expression storage space with attacker supplied data.

The target system needs a sufficient amount of memory to allocate partial expansions of the nested quantifiers prior to the overflow occurring. This requirement is unlikely to be met on 64-bit systems.

Discovered by: ManhND of The Tarantula Team, VinCSS (a member of Vingroup).

[CVE-2020-10878] Integer overflow via malformed bytecode produced by a crafted regular expression

Integer overflows in the calculation of offsets between instructions for the regular expression engine could cause corruption of the intermediate language state of a compiled regular expression. An attacker could abuse this behaviour to insert instructions into the compiled form of a Perl regular expression.

Discovered by: Hugo van der Sanden and Slaven Rezic.

[CVE-2020-12723] Buffer overflow caused by a crafted regular expression

Recursive calls to "S_study_chunk()" by Perl's regular expression compiler to optimize the intermediate language representation of a regular expression could cause corruption of the intermediate language state of a compiled regular expression.

Discovered by: Sergey Aleynikov.

Additional Note

An application written in Perl would only be vulnerable to any of the above flaws if it evaluates regular expressions supplied by the attacker. Evaluating regular expressions in this fashion is known to be dangerous since the regular expression engine does not protect against denial of service attacks in this usage scenario.

Incompatible Changes

There are no changes intentionally incompatible with Perl 5.30.2. If any exist, they are bugs, and we request that you submit a report. See "Reporting Bugs" below.

Modules and Pragmata

Updated Modules and Pragmata

- Module::CoreList has been upgraded from version 5.20200314 to 5.20200601_30.

Testing

Tests were added and changed to reflect the other additions and changes in this release.

Acknowledgements

Perl 5.30.3 represents approximately 3 months of development since Perl 5.30.2 and contains approximately 1,100 lines of changes across 42 files from 7 authors.

Excluding auto-generated files, documentation and release tools, there were approximately 350 lines of changes to 8 .pm, .t, .c and .h files.

Perl continues to flourish into its fourth decade thanks to a vibrant community of users and developers. The following people are known to have contributed the improvements that became Perl 5.30.3:

Chris ’BinGOs’ Williams, Hugo van der Sanden, John Lightsey, Karl Williamson, Nicolas R., Sawyer X, Steve Hay.

The list above is almost certainly incomplete as it is automatically generated from version control history. In particular, it does not include the names of the (very much appreciated) contributors who reported issues to the Perl bug tracker.

Many of the changes included in this version originated in the CPAN modules included in Perl’s core. We’re grateful to the entire CPAN community for helping Perl to flourish.

For a more complete list of all of Perl’s historical contributors, please see the *AUTHORS* file in the Perl source distribution.

Reporting Bugs

If you find what you think is a bug, you might check the perl bug database at <https://github.com/Perl/perl5/issues>. There may also be information at <https://www.perl.org/>, the Perl Home Page.

If you believe you have an unreported bug, please open an issue at

<https://github.com/Perl/perl5/issues>. Be sure to trim your bug down to a tiny but sufficient test case.

If the bug you are reporting has security implications which make it inappropriate to send to a public issue tracker, then see "SECURITY VULNERABILITY CONTACT INFORMATION" in perlsec for details of how to report the issue.

Give Thanks

If you wish to thank the Perl 5 Porters for the work we had done in Perl 5, you can do so by running the "perlthanks" program:

```
perlthanks
```

This will send an email to the Perl 5 Porters list with your show of thanks.

SEE ALSO

The *Changes* file for an explanation of how to view exhaustive details on what changed.

The *INSTALL* file for how to build Perl.

The *README* file for general stuff.

The *Artistic* and *Copying* files for copyright information.