NAME

perl5144delta - what is new for perl v5.14.4

DESCRIPTION

This document describes differences between the 5.14.3 release and the 5.14.4 release.

If you are upgrading from an earlier release such as 5.12.0, first read *perl5140delta*, which describes differences between 5.12.0 and 5.14.0.

Core Enhancements

No changes since 5.14.0.

Security

This release contains one major, and medium, and a number of minor security fixes. The latter are included mainly to allow the test suite to pass cleanly with the clang compiler's address sanitizer facility.

CVE-2013-1667: memory exhaustion with arbitrary hash keys

With a carefully crafted set of hash keys (for example arguments on a URL), it is possible to cause a hash to consume a large amount of memory and CPU, and thus possibly to achieve a Denial-of-Service.

This problem has been fixed.

memory leak in Encode

The UTF-8 encoding implementation in Encode.xs had a memory leak which has been fixed.

[perl #111594] Socket::unpack_sockaddr_un heap-buffer-overflow

A read buffer overflow could occur when copying `sockaddr` buffers. Fairly harmless.

This problem has been fixed.

[perl #111586] SDBM_File: fix off-by-one access to global ".dir"

An extra byte was being copied for some string literals. Fairly harmless.

This problem has been fixed.

off-by-two error in List::Util

A string literal was being used that included two bytes beyond the end of the string. Fairly harmless.

This problem has been fixed.

[perl #115994] fix segv in regcomp.c:S_join_exact()

Under debugging builds, while marking optimised-out regex nodes as type `OPTIMIZED`, it could treat blocks of exact text as if they were nodes, and thus SEGV. Fairly harmless.

This problem has been fixed.

[perl #115992] PL_eval_start use-after-free

The statement `local $[;`, when preceded by an `eval`, and when not part of an assignment, could crash. Fairly harmless.

This problem has been fixed.

wrap-around with IO on long strings

Reading or writing strings greater than 2**31 bytes in size could segfault due to integer wraparound.

This problem has been fixed.

Incompatible Changes

There are no changes intentionally incompatible with 5.14.0. If any exist, they are bugs and reports are welcome.

Deprecations

There have been no deprecations since 5.14.0.

Modules and Pragmata

New Modules and Pragmata

None

Updated Modules and Pragmata

The following modules have just the minor code fixes as listed above in *Security* (version numbers have not changed):

Socket

SDBM_File

List::Util

Encode has been upgraded from version 2.42_01 to version 2.42_02.

Module::CoreList has been updated to version 2.49_06 to add data for this release.

Removed Modules and Pragmata

None.

Documentation

New Documentation

None.

Changes to Existing Documentation

None.

Diagnostics

No new or changed diagnostics.

Utility Changes

None

Configuration and Compilation

No changes.

Platform Support

New Platforms

None.

Discontinued Platforms

None.

Platform-Specific Notes

VMS

5.14.3 failed to compile on VMS due to incomplete application of a patch series that allowed `userelocatableinc` and `usesitecustomize` to be used simultaneously. Other platforms were not affected and the problem has now been corrected.

Selected Bug Fixes

- In Perl 5.14.0, `$tainted ~~ @array` stopped working properly. Sometimes it would erroneously fail (when `$tainted` contained a string that occurs in the array *after* the first element) or erroneously succeed (when `undef` occurred after the first element) [perl #93590].

Known Problems

None.

Acknowledgements

Perl 5.14.4 represents approximately 5 months of development since Perl 5.14.3 and contains approximately 1,700 lines of changes across 49 files from 12 authors.

Perl continues to flourish into its third decade thanks to a vibrant community of users and developers. The following people are known to have contributed the improvements that became Perl 5.14.4:

Andy Dougherty, Chris 'BinGOs' Williams, Christian Hansen, Craig A. Berry, Dave Rolsky, David Mitchell, Dominic Hargreaves, Father Chrysostomos, Florian Ragwitz, Reini Urban, Ricardo Signes, Yves Orton.

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.

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 articles recently posted to the comp.lang.perl.misc newsgroup and the perl bug database at http://rt.perl.org/perlbug/ . There may also be information at http://www.perl.org/ , the Perl Home Page.

If you believe you have an unreported bug, please run the *perlbug* program included with your release. Be sure to trim your bug down to a tiny but sufficient test case. Your bug report, along with the output of `perl -V`, will be sent off to perlbug@perl.org to be analysed by the Perl porting team.

If the bug you are reporting has security implications, which make it inappropriate to send to a publicly archived mailing list, then please send it to perl5-security-report@perl.org. This points to a closed subscription unarchived mailing list, which includes all the core committers, who be able to help assess the impact of issues, figure out a resolution, and help co-ordinate the release of patches to mitigate or fix the problem across all platforms on which Perl is supported. Please only use this address for security issues in the Perl core, not for modules independently distributed on CPAN.

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.