NAME

perl5125delta - what is new for perl v5.12.5

DESCRIPTION

This document describes differences between the 5.12.4 release and the 5.12.5 release.

If you are upgrading from an earlier release such as 5.12.3, first read perl5124delta, which describes differences between 5.12.3 and 5.12.4.

Security

"Encode" decode_xs n-byte heap-overflow (CVE-2011-2939)

A bug in "Encode" could, on certain inputs, cause the heap to overflow. This problem has been corrected. Bug reported by Robert Zacek.

"File::Glob::bsd_glob()" memory error with GLOB_ALTDIRFUNC (CVE-2011-2728).

Calling "File::Glob::bsd_glob" with the unsupported flag GLOB_ALTDIRFUNC would cause an access violation / segfault. A Perl program that accepts a flags value from an external source could expose itself to denial of service or arbitrary code execution attacks. There are no known exploits in the wild. The problem has been corrected by explicitly disabling all unsupported flags and setting unused function pointers to null. Bug reported by Clement Lecigne.

Heap buffer overrun in ’x’ string repeat operator (CVE-2012-5195)

Poorly written perl code that allows an attacker to specify the count to perl’s ’x’ string repeat operator can already cause a memory exhaustion denial-of-service attack. A flaw in versions of perl before 5.15.5 can escalate that into a heap buffer overrun; coupled with versions of glibc before 2.16, it possibly allows the execution of arbitrary code.

This problem has been fixed.

Incompatible Changes

There are no changes intentionally incompatible with 5.12.4. If any exist, they are bugs and reports are welcome.

Modules and Pragmata

Updated Modules

B::Concise

B::Concise no longer produces mangled output with the **-tree** option [perl #80632].

charnames

A regression introduced in Perl 5.8.8 has been fixed, that caused charnames::viacode(0) to return "undef" instead of the string "NULL" [perl #72624].

Encode has been upgraded from version 2.39 to version 2.39_01.

See "Security".

File::Glob has been upgraded from version 1.07 to version 1.07_01.

See "Security".

Unicode::UCD

The documentation for the "upper" function now actually says "upper", not "lower".

Module::CoreList

Module::CoreList has been updated to version 2.50_02 to add data for this release.

Changes to Existing Documentation

perlebcdic

The perlebcdic document contains a helpful table to use in "tr///" to convert between EBCDIC and Latin1/ASCII. Unfortunately, the table was the inverse of the one it describes. This has been corrected.

perlunicode

The section on User-Defined Case Mappings had some bad markup and unclear sentences, making parts of it unreadable. This has been rectified.

perluniprops

This document has been corrected to take non-ASCII platforms into account.

Installation and Configuration Improvements

Platform Specific Changes

Mac OS X

There have been configuration and test fixes to make Perl build cleanly on Lion and Mountain Lion.

NetBSD

The NetBSD hints file was corrected to be compatible with NetBSD 6.*

Selected Bug Fixes

- "chop" now correctly handles characters above "\x{7fffffff}" [perl #73246].

- "($<,$>) = (...)" stopped working properly in 5.12.0. It is supposed to make a single "setreuid()" call, rather than calling "setruid()" and "seteuid()" separately. Consequently it did not work properly. This has been fixed [perl #75212].

- Fixed a regression of **kill()** when a match variable is used for the process ID to kill [perl #75812].

- "UNIVERSAL::VERSION" no longer leaks memory. It started leaking in Perl 5.10.0.

- The C-level "my_strftime" functions no longer leaks memory. This fixes a memory leak in "POSIX::strftime" [perl #73520].

- "caller" no longer leaks memory when called from the DB package if @DB::args was assigned to after the first call to "caller". Carp was triggering this bug [perl #97010].

- Passing to "index" an offset beyond the end of the string when the string is encoded internally in UTF8 no longer causes panics [perl #75898].

- Syntax errors in "(?{...})" blocks in regular expressions no longer cause panic messages [perl #2353].

- Perl 5.10.0 introduced some faulty logic that made "U*" in the middle of a pack template equivalent to "U0" if the input string was empty. This has been fixed [perl #90160].

Errata

split() and @_

split() no longer modifies @_ when called in scalar or void context. In void context it now produces a "Useless use of split" warning. This is actually a change introduced in perl 5.12.0, but it was missed from that release's perl5120delta.

Acknowledgements

Perl 5.12.5 represents approximately 17 months of development since Perl 5.12.4 and contains approximately 1,900 lines of changes across 64 files from 18 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 5.12.5:

Andy Dougherty, Chris 'BinGOs' Williams, Craig A. Berry, David Mitchell, Dominic Hargreaves,

Father Chrysostomos, Florian Ragwitz, George Greer, Goro Fuji, Jesse Vincent, Karl Williamson, Leon Brocard, Nicholas Clark, Rafael Garcia-Suarez, Reini Urban, Ricardo Signes, Steve Hay, Tony Cook.

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 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.