

NAME

perl5342delta - what is new for perl v5.34.2

DESCRIPTION

This document describes differences between the 5.34.1 release and the 5.34.2 release.

If you are upgrading from an earlier release such as 5.34.0, first read perl5341delta, which describes differences between 5.34.0 and 5.34.1.

Security

This release fixes the following security issues.

CVE-2023-47038 - Write past buffer end via illegal user-defined Unicode property

This vulnerability was reported directly to the Perl security team by Nathan Mills "the.true.nathan.mills@gmail.com".

A crafted regular expression when compiled by perl 5.30.0 through 5.38.0 can cause a one-byte attacker controlled buffer overflow in a heap allocated buffer.

CVE-2023-47039 - Perl for Windows binary hijacking vulnerability

This vulnerability was reported to the Intel Product Security Incident Response Team (PSIRT) by GitHub user ycdxsb <<https://github.com/ycdxsb/WindowsPrivilegeEscalation>>. PSIRT then reported it to the Perl security team.

Perl for Windows relies on the system path environment variable to find the shell ("cmd.exe"). When running an executable which uses Windows Perl interpreter, Perl attempts to find and execute "cmd.exe" within the operating system. However, due to path search order issues, Perl initially looks for cmd.exe in the current working directory.

An attacker with limited privileges can exploit this behavior by placing "cmd.exe" in locations with weak permissions, such as "C:\ProgramData". By doing so, when an administrator attempts to use this executable from these compromised locations, arbitrary code can be executed.

Acknowledgements

Perl 5.34.2 represents approximately 1 month of development since Perl 5.34.1 and contains approximately 3,700 lines of changes across 40 files from 4 authors.

Excluding auto-generated files, documentation and release tools, there were approximately 2,800 lines of changes to 9 .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 5.34.2:

Karl Williamson, Paul Evans, 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 perl bug database at <https://github.com/Perl/perl5/issues>. There may also be information at <http://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.