Alpine Linux - Bug #9728

Bug # 9726 (Closed): perl: Multiple vulnerabilities (CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314)

[3.8] perl: Multiple vulnerabilities (CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314)

12/04/2018 10:06 AM - Alicha CH

Status:	Closed	**Start date:**	12/04/2018
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314

Description

CVE-2018-18311: Integer overflow leading to buffer overflow

A flaw was found in Perl versions 5.8.0 through 5.28. An Integer overflow leading to buffer overflow in Perl_my_setenv function in util.c

Fixed In Version:

perl 5.29.1, perl 5.26.3

Reference:

https://rt.perl.org/Public/Bug/Display.html?id=133204

Patch:

https://github.com/Perl/perl5/commit/34716e2a6ee2af96078d62b065b7785c001194be
Introduced by: https://perl5.git.perl.org/perl.git/commitdiff/e658793210bbe632a5e80a876acfcd0984c46b87

CVE-2018-18312: Heap-buffer-overflow write / reg_node overrun

A flaw was found in Perl versions 5.18 through 5.26. A Heap-buffer-overflow write / reg_node overrun

Fixed In Version:

perl 5.26.3, perl 5.28.1

References:

https://rt.perl.org/Ticket/Display.html?id=133423
https://security-tracker.debian.org/tracker/CVE-2018-18312

CVE-2018-18313: Heap-buffer-overflow read in regcomp.c

A flaw was found in Perl versions 5.22 through 5.26. Heap-buffer-overflow read in regcomp.c

Fixed In Version:

perl 5.26.3, perl 5.28.1

Reference:

https://rt.perl.org/Public/Bug/Display.html?id=133192

Patch:

https://github.com/Perl/perl5/commit/43b2f4ef399e2fd7240b4eeb0658686ad95f8e62

CVE-2018-18314: Heap-based buffer overflow

A flaw was found in Perl versions 5.18 through 5.28. A Heap-based buffer overflow

Fixed In Version:

perl 5.26.3, perl 5.28.1

Reference:

https://rt.perl.org/Public/Bug/Display.html?id=131649

Patch:

https://github.com/Perl/perl5/commit/19a498a461d7c81ae3507c450953d1148efecf4f

Associated revisions

Revision d64c1df5 - 12/04/2018 02:47 PM - Natanael Copa

main/perl: security upgrade to 5.26.3

CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314

fixes #9728

History

#1 - 12/04/2018 04:27 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:d64c1df53210ad5f3d6666da967b2628cf0eb172.

#2 - 12/06/2018 09:46 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed