Bug 717920 (CVE-2019-20838, CVE-2020-14155) - <dev-libs/libpcre-8.44: Multiple vulnerabilities (CVE-2019-20838, CVE-2020-14155)

Status: RESOLVED FIXED
Alias: CVE-2019-20838, CVE-2020-14155
Product: Gentoo Security
Component: Vulnerabilities (show other bugs)
Hardware: All Linux
Importance: Normal minor
Assignee: Gentoo Security
URL: http://www.pcre.org/original/changelo...
Whiteboard: B3 [noglsa cve]
Keywords:
Depends on:
Blocks:

Reported: 2020-04-17 17:23 UTC by Sam James
Modified: 2020-12-23 16:27 UTC (History)
CC List: 1 user (show)
See Also:
Flags: nattka: sanity-check+

Attachments
Add an attachment (proposed patch, testcase, etc.)

Note
You need to log in before you can comment on or make changes to this bug.

Note: Please do not mark this bug as resolved after bumping or stabilizing. The Security Team will take care of that. Thanks.

Sam James AT InFra Dev Sec **2020-04-17 17:23:29 UTC** Description

```
Quoting from ChangeLog (8.44):
"6. Check the size of the number after (?C as it is read, in order to avoid
integer overflow."
"7. Tidy up left shifts to avoid sanitize warnings; also fix one NULL deference
in pcretest."


Quoting from ChangeLog (8.43):
"7. Fix subject buffer overread in JIT when UTF is disabled and \X or \R has
a greater than 1 fixed quantifier. This issue was found by Yunho Kim."
```

Sam James AT InFra Dev Sec **2020-04-17 17:23:54 UTC** Comment 1

```
@maintainer(s), please advise if ready for stabilisation, or call yourself
```

Sam James AT InFra Dev Sec **2020-06-04 17:00:43 UTC** Comment 2

ping

jylipeng **2020-06-29 07:51:03 UTC** Comment 3

@Sam James hi,I found this testcase could reproduce the bug in pcre2, but in pcre 8.42, I could not reproduce it.

/\X*/
    \xF3aaa\xE4\xEA\xEB\XFEa

Could you provide the suitable testcase for me to veritfy this change?

Sam James AT InFra Dev Sec **2020-08-19 09:06:38 UTC** Comment 4

arm64 done

Agostino Sarubbo Dev **2020-08-21 15:27:43 UTC** Comment 5

arm stable

Agostino Sarubbo Dev **2020-08-22 05:50:55 UTC** Comment 6

x86 stable

Agostino Sarubbo Dev **2020-08-22 11:26:48 UTC** Comment 7

amd64 stable

Sam James AT InFra Dev Sec **2020-08-29 04:44:12 UTC** Comment 8

ppc done

Sergei Trofimovich (RETIRED) Dev **2020-08-29 07:57:32 UTC** Comment 9

sparc stable

Sergei Trofimovich (RETIRED) Dev **2020-09-04 11:54:04 UTC** Comment 10

commit 4b467aaca13059e5b4438bc98de65f00c45dc8f1
Author: Sam James <sam@gentoo.org>
Date: Thu Sep 3 23:42:29 2020 +0000

    dev-libs/libpcre: ppc64 stable (~~bug #717920~~)

Sergei Trofimovich (RETIRED) Dev **2020-09-06 08:18:31 UTC** Comment 11

hppa stable

Sam James AT InFra Dev Sec **2020-09-06 14:21:44 UTC** Comment 12

s390: ping

Agostino Sarubbo Dev **2020-09-18 08:11:24 UTC** Comment 13

s390 stable.

Maintainer(s), please cleanup.
Security, please vote.

Larry the Git Cow Dev **2020-09-18 10:30:14 UTC** Comment 14

The bug has been referenced in the following commit(s):

https://gitweb.gentoo.org/repo/gentoo.git/commit/?id=577e461933395f3e973e0c153e3a1080cdf0a284

commit 577e461933395f3e973e0c153e3a1080cdf0a284
Author: Lars Wendler <polynomial-c@gentoo.org>
AuthorDate: 2020-09-18 10:29:29 +0000
Commit: Lars Wendler <polynomial-c@gentoo.org>
CommitDate: 2020-09-18 10:30:10 +0000

    dev-libs/libpcre: Security cleanup

    Bug: https://bugs.gentoo.org/717920
    Package-Manager: Portage-3.0.7, Repoman-3.0.1
    Signed-off-by: Lars Wendler <polynomial-c@gentoo.org>

 dev-libs/libpcre/Manifest | 2 -
 dev-libs/libpcre/libpcre-8.42.ebuild | 96 ----------------------------------
 dev-libs/libpcre/libpcre-8.43.ebuild | 96 ----------------------------------
 3 files changed, 194 deletions(-)

Thomas Deutschmann (RETIRED) Dev **2020-12-23 16:27:08 UTC** Comment 15

GLSA Vote: No

Repository is clean, all done!

Format For Printing - XML - Clone This Bug - Clone In The Same Product - Top of page