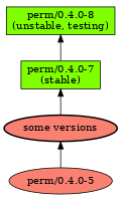
Debian Bug report logs - #993019
perm -- Buffer overflows



Package: perm; Maintainer for perm is Debian Med Packaging Team <debian-med-packaging@lists.alioth.debian.org>; Source for perm is src:perm (PTS, buildd, popcon).

Reported by: Nilesh Patra <nilesh@debian.org>

Date: Thu, 26 Aug 2021 12:12:02 UTC

Severity: normal

Found in version perm/0.4.0-5

Fixed in version perm/0.4.0-7

Done: Nilesh Patra <nilesh@debian.org>

Reply or subscribe to this bug.

Toggle useless messages

View this report as an mbox folder, status mbox, maintainer mbox

---

Message #5 received at submit@bugs.debian.org (full text, mbox, reply):

From: Nilesh Patra <nilesh@debian.org>
To: Debian Bug Tracking System <submit@bugs.debian.org>
Subject: perm -- Buffer overflows
Date: Thu, 26 Aug 2021 17:40:13 +0530

```
Package: perm

Version: 0.4.0-5

Severity: normal

X-Debbugs-Cc: nilesh@debian.org, utkarsh@debian.org


Hi,


This bug report is being done as a reference point for perm to be

processed with the corresponding CVE (also as a reference point for

Mitre)


This bug was actually discovered very publically on a mailing list

itself[1] and here is the unblock bug[2]


So, automated tests (autopkgtests) were added to perm, to run on a

test data that can be found here[3]. On propagarting a hardening flag,

particularly -D_FORTIFY_SOURCE=2 this started to give buffer overflow

errors, as can be seen here[4]


I did a patch[5], and uploaded the fixed version 0.4.0-7 which fixes the

issue at hand[6].


Now, when I tried contacting upstream, I realised that upstream sources

are not present anywhere, and probably that was the case since several

years, as is also apparent from the copyright file[7]


I did see a email address there (Yangho Chen et al. <yanghoch@usc.edu>), and I sent in an email there asking for

it and also reporting the security issue, but by far there has been no

response for several days and I think it is safe to assume that the

upstream development for this software is dead.


Overall, this software was in fact vulnerable, and the vulnerability can
```

be tested with running:

```
$ perm Ref.fasta Reads.fasta -v 100 -A -o out.sam
```

as given in test test data linked below, and the corresponding CI

[1]: https://lists.debian.org/debian-med/2021/08/msg00016.html

[2]: https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=991841

[3]: https://salsa.debian.org/med-team/perm/-/tree/master/debian/tests/data

[4]: https://salsa.debian.org/med-team/perm/-/jobs/1788156

[5]: https://salsa.debian.org/med-team/perm/-/blob/master/debian/patches/fix-buffer-overflow.patch

[6]: https://salsa.debian.org/med-team/perm/-/jobs/1789569

[7]: https://salsa.debian.org/med-team/perm/-/blob/master/debian/copyright#L3

Nilesh

Marked as fixed in versions perm/0.4.0-7. Request was from Nilesh Patra <nilesh@debian.org> to control@bugs.debian.org. (Thu, 26 Aug 2021 12:36:03 GMT) (**full text**, **mbox**, **link**).

Reply sent to Nilesh Patra <nilesh@debian.org>:

You have taken responsibility. (Sun, 04 Dec 2022 15:51:07 GMT) (**full text**, **mbox**, **link**).

Message #12 received at 993019-done@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Nilesh Patra <nilesh@debian.org>
To: 993019-done@bugs.debian.org
Subject: Re: perm -- Buffer overflows
Date: Sun, 4 Dec 2022 21:17:14 +0530

[**Message part 1** (text/plain, inline)]

The CVE details for this has been published by MITRE

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38172

Closing.

--

Best,

Nilesh

[**signature.asc** (application/pgp-signature, inline)]

Send a report that **this bug log contains spam**.
