Debian Bug report logs - #981404
compressed file is world readable, while zstd is running

Package: zstd; Maintainer for zstd is RPM packaging team <team+pkg-rpm@tracker.debian.org>; Source for zstd is src:libzstd (PTS, buildd, popcon).

Reported by: Harald Dunkel <harri@afaics.de>

Date: Sat, 30 Jan 2021 16:45:02 UTC

Severity: *critical*

Tags: fixed-upstream, patch, upstream

Found in versions libzstd/1.3.8+dfsg-3, libzstd/1.1.2-1

Fixed in versions libzstd/1.4.8+dfsg-1, libzstd/1.3.8+dfsg-3+deb10u1

Done: Étienne Mollier <etienne.mollier@mailoo.org>

Bug is archived. No further changes may be made.

Forwarded to https://github.com/facebook/zstd/issues/1630

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: Harald Dunkel <harri@afaics.de>
To: Debian Bug Tracking System <submit@bugs.debian.org>
Subject: compressed file is world readable, while zstd is running
Date: Sat, 30 Jan 2021 17:34:45 +0100

Package: zstd

Version: 1.3.8+dfsg-3

Severity: critical

Compressing a large file with restricted access permissions a new,

world readable file is created, revealing the contents of the

uncompressed file. Sample:

```
# whoami
root
# zstd -q -13 -T8 sample.dmp &> zstd.log &
:
:
# ls -al
total 385983012
drwxr-xr-x  2 root    root          4096 Jan 30 16:01 .
drwxr-xr-x 35 root    root          4096 Jan 30 15:39 ..
-rw-------  1 oracle  users 279265214464 Jan 29 22:02 sample.dmp
-rw-r--r--  1 root    root  115981336576 Jan 30 16:25 sample.dmp.zst
-rw-r--r--  1 root    root             0 Jan 30 16:01 zstd.log
:
:
[1]+  Done                    zstd -q -13 -T8 sample.dmp &> zstd.log
# md5sum sample.dmp.zst
5a3d3401e8e46483659e820f96ad0ef0  sample.dmp.zst
```

An attacker might be able to open(2) the file while zstd is still

running, wait for zstd to complete its job, and then read(2) the

whole file:

```
% whoami
attacker
% ls -al
total 465071584
drwxr-xr-x  2 root    root          4096 Jan 30 16:01 .
drwxr-xr-x 35 root    root          4096 Jan 30 15:39 ..
-rw-------  1 oracle  users 279265214464 Jan 29 22:02 sample.dmp
-rw-r--r--  1 root    root  196968022016 Jan 30 16:41 sample.dmp.zst
-rw-r--r--  1 root    root             0 Jan 30 16:01 zstd.log
% md5sum sample.dmp.zst
^Z
[1]+  Stopped                 md5sum sample.dmp.zst
:
:
% ls -al
total 475580484
drwxr-xr-x  2 root    root          4096 Jan 30 16:01 .
drwxr-xr-x 35 root    root          4096 Jan 30 15:39 ..
-rw-------  1 oracle  users 279265214464 Jan 29 22:02 sample.dmp
-rw-------  1 oracle  users 207729131801 Jan 29 22:02 sample.dmp.zst
-rw-r--r--  1 root    root             0 Jan 30 16:01 zstd.log

% fg
md5sum sample.dmp.zst
5a3d3401e8e46483659e820f96ad0ef0  sample.dmp.zst
%
```

In this sample session the attacker got the correct md5sum, just for
demonstation purposes. Hi could have created his own private copy in
the same way.

This makes zstd unusable for me.

Regards
Harri

Message #10 received at 981404@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Étienne Mollier <etienne.mollier@mailoo.org>
To: 981404@bugs.debian.org
Subject: Re: [Debian-med-packaging] Bug#981404: compressed file is world readable, while zstd is running
Date: Mon, 1 Feb 2021 22:57:15 +0100

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

Control: fixed -1 1.4.8+dfsg-1
Control: tag -1 patch

Greetings,

This critical issue is affecting Stable. Permissions at compression time are inherited from umask, this may be too relaxed when handling sensitive files.

Fortunately, this seems to have been fixed upstream around version 1.4.1. Debian Sid is not affected anymore as far as I can see. I identified the few commits[1,2,3,4] from Mike Swanson and Yann Collet which solved the issue.

[1] https://github.com/facebook/zstd/commit/3968160a916a759c3d3418da533e1b4f8b795343

[2] https://github.com/facebook/zstd/commit/af80f6dfacafcc2c916ecd57731107221e1f9986

[3] https://github.com/facebook/zstd/commit/8b6d96827c24dd09109830272f413254833317d9

[4] https://github.com/facebook/zstd/commit/7aaac3f69c1e0102099c192639017e660e88b4bf

After some folding, I obtained the following patch, with which I could derive a fixed version of zstd 1.3.8 for Buster:

```
-------8<--------------8<--------------8<--------------8<-------
--- libzstd.orig/programs/fileio.c
+++ libzstd/programs/fileio.c
@@ -482,8 +482,14 @@
     }   }

     {   FILE* const f = fopen( dstFileName, "wb" );
-        if (f == NULL)
+        if (f == NULL) {
             DISPLAYLEVEL(1, "zstd: %s: %s\n", dstFileName, strerror(errno));
+        } else if (srcFileName != NULL
+                   && strcmp (srcFileName, stdinmark)
+                   && strcmp(dstFileName, nulmark) ) {
+                /* reduce rights on newly created dst file while compression is ongoing */
+            chmod(dstFileName, 00600);
+        }
         return f;
     }
 }
-------8<--------------8<--------------8<--------------8<-------
```

Side note to Debian Med, I know the package is transitionning to pkg-rpm team, and I am not super comfortable yet preparing an upload to Stable[5], so I'm just providing a proposal of patch as a starter.

[5] https://www.debian.org/doc/manuals/developers-reference/pkgs.en.html#special-case-uploads-to-the-stable-and-oldstable-distributions

Kind Regards,

--

Étienne Mollier <etienne.mollier@mailoo.org>

Fingerprint: 8f91 b227 c7d6 f2b1 948c 8236 793c f67e 8f0d 11da

Sent from /dev/pts/2, please excuse my verbosity.

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

Marked as fixed in versions libzstd/1.4.8+dfsg-1. Request was from Étienne Mollier <etienne.mollier@mailoo.org> to 981404-submit@bugs.debian.org. (Mon, 01 Feb 2021 21:58:12 GMT) (**full text**, **mbox**, **link**).

Added tag(s) patch. Request was from Étienne Mollier <etienne.mollier@mailoo.org> to 981404-submit@bugs.debian.org. (Mon, 01 Feb 2021 21:58:12 GMT) (**full text**, **mbox**, **link**).

Set Bug forwarded-to-address to 'https://github.com/facebook/zstd/issues/1630'. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Wed, 03 Feb 2021 21:39:02 GMT) (**full text**, **mbox**, **link**).

Added tag(s) upstream and fixed-upstream. Request was from Salvatore Bonaccorso <carnil@debian.org> to control@bugs.debian.org. (Wed, 03 Feb 2021 21:39:03 GMT) (**full text**, **mbox**, **link**).

Reply sent to Étienne Mollier <etienne.mollier@mailoo.org>:

You have taken responsibility. (Wed, 10 Feb 2021 22:33:03 GMT) (**full text**, **mbox**, **link**).

Message #23 received at 981404-close@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Debian FTP Masters <ftpmaster@ftp-master.debian.org>
To: 981404-close@bugs.debian.org
Subject: Bug#981404: fixed in libzstd 1.3.8+dfsg-3+deb10u1
Date: Wed, 10 Feb 2021 22:32:10 +0000

```
Source: libzstd
Source-Version: 1.3.8+dfsg-3+deb10u1
Done: Étienne Mollier <etienne.mollier@mailoo.org>

We believe that the bug you reported is fixed in the latest version of
libzstd, which is due to be installed in the Debian FTP archive.

A summary of the changes between this version and the previous one is
attached.

Thank you for reporting the bug, which will now be closed.  If you
have further comments please address them to 981404@bugs.debian.org,
and the maintainer will reopen the bug report if appropriate.

Debian distribution maintenance software
pp.
Étienne Mollier <etienne.mollier@mailoo.org> (supplier of updated libzstd package)

(This message was generated automatically at their request; if you
believe that there is a problem with it please contact the archive
administrators by mailing ftpmaster@ftp-master.debian.org)


-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Format: 1.8
Date: Mon, 01 Feb 2021 20:36:53 +0100
Source: libzstd
Architecture: source
Version: 1.3.8+dfsg-3+deb10u1
Distribution: buster-security
Urgency: high
Maintainer: Debian Med Packaging Team <debian-med-packaging@lists.alioth.debian.org>
Changed-By: Étienne Mollier <etienne.mollier@mailoo.org>
```

```
Closes: 981404
Changes:
 libzstd (1.3.8+dfsg-3+deb10u1) buster-security; urgency=high
 .
   * Team upload.
   * When a file with restricted permissions is compressed, the resulting file
     inherits the umask of the user for the time of the compression.  This will
     usually lead to surprising and too relaxed permissions.  This update adds
     fix-file-permissions-on-compression.patch to make sure the compressed file
     is not group or world readable for the duration of the compression.
     Closes: #981404
Checksums-Sha1:
 909d33d6118457384ba8e90fe7b319ed70f58706 2292 libzstd_1.3.8+dfsg-3+deb10u1.dsc
 4283d7fd3abb54208784456b8883c4c90d760940 1299276 libzstd_1.3.8+dfsg.orig.tar.xz
 4ebdb2e9974bd2945008da1a3bc6d8fc1e0ca4bc 10864 libzstd_1.3.8+dfsg-3+deb10u1.debian.tar.xz
 7fefa795f057209c4624f79555b2e960f9b52311 7563 libzstd_1.3.8+dfsg-3+deb10u1_amd64.buildinfo
Checksums-Sha256:
 6ce2a1aafcde927492ac01e89488dc1640fc1dab8be8ded1947b3c06a421d98c 2292 libzstd_1.3.8+dfsg-3+deb10u1.dsc
 03851f2c26ffbf1d43633df3f98966f3c62e698e91ef4dc90523915bc934e5f7 1299276 libzstd_1.3.8+dfsg.orig.tar.xz
 0109ff8e2b23662da58fe018959844c264985345a9b03bdb2213b760de87611b 10864 libzstd_1.3.8+dfsg-3+deb10u1.debian.tar.xz
 32ffe444a0584d9622510c11222e27f9dad7b0c4bc4436eb83917ea1b2e6bea4 7563 libzstd_1.3.8+dfsg-3+deb10u1_amd64.buildinfo
Files:
 83019be1592cf47a45a3b206c96a776a 2292 libs optional libzstd_1.3.8+dfsg-3+deb10u1.dsc
 be6c01a65c48b62e151dd0972a36e995 1299276 libs optional libzstd_1.3.8+dfsg.orig.tar.xz
 aa6dfd0f7bcf8b7bee01613540800fe1 10864 libs optional libzstd_1.3.8+dfsg-3+deb10u1.debian.tar.xz
 bc263ca409b530dcf48154928f71690b 7563 libs optional libzstd_1.3.8+dfsg-3+deb10u1_amd64.buildinfo

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEsaUesned0BdDzBm6HPeSERtSKLAFAmAhotsACgkQHPeSERtS
KLBNnQ//eMzoHIEaIcfFb7KrxETltbOTWnXG5ml6CjV/gIrtGe+aLshUJTa8Uek9
ABaVXd1ij9yh81f6Hx1MsKYk66EbYz33TVV3UwjTgDjysKqH9g2SgZ6Gm3Wb1EQE
NOAu0BNTTtdw6KPI7Rn3URMR6Ab6rnu93OXOo8uL8f0lqVhWqnu8Vvw+pBoVBnT5
SH4Q98GdIjxitKvBIuTKGcqCgV25lUb+Ccg6QmkWDrRRL/ESxGrC4cj487aoVLem
v2WxQpQlyOrI7/SMsG24Tf1Bp+wMCiDptiv/LVkJOQF3YtQWtAv+EUNQDAg3+OAv
H/Z3qq+qIGx6+yS/yAPPd8CchZVMAG6Gi/25PniwJ9/BPjIXBUL3vj8DabyoEJyN
cWkd+SavLPjPtkvPZCdA1NqK0V0UtMp0/ET111pTfdGXxdKxLhrL1IOHyymH4FZ6
+aqNbc90fophz8+DtjxvWPN7MH+llrako1TS3tvuJuGOQdjLtjE1zowo10KTDeJd
D8lI8eRQ6bD+CdlUC6o2RJ5lWh2oiRaOx1wDSHdGij4jYDxtuVV3C7HlT0tFyYiP
p2HZe+fz0ekMTTjJkJjoqsGw80n6yM6UocMfDphnqrPlNAR9GcEUFXy8eeny3i4v
H3CZSV6OfaxSK7N/KCCqPWDKj9VScGC5R4wp4CqIiTmByxapXdY=
=9+fx
-----END PGP SIGNATURE-----
```

Message #28 received at 981404@bugs.debian.org (**full text**, **mbox**, **reply**):

From: wferi@niif.hu
To: 981404@bugs.debian.org
Subject: Fix seems incomplete
Date: Thu, 11 Feb 2021 11:26:47 +0100

Hi,

The patch in this bug report very much shrinks the window of the vulnerability, but doesn't close it completely: the file is still created with default permissions, then chmodded as a separate step. It's hard, but not impossible to still win the race and open the file before the chmod, enabling the same attack. I recommend something like

```
fd = open(dstFileName, O_WRONLY|O_CREAT|O_EXCL, 0600);
if (fd != -1)
    f = fdopen( fd, "wb" );
if (fd == -1 || f == NULL)
    DISPLAYLEVEL(1, "zstd: %s: %s\n", dstFileName, strerror(errno));
return f;
```

for example.

--

Regards,

Feri

Message #33 received at 981404@bugs.debian.org (**full text**, **mbox**, **reply**):

From: Salvatore Bonaccorso <carnil@debian.org>
To: wferi@niif.hu, 981404@bugs.debian.org
Cc: 982519@bugs.debian.org
Subject: Re: Bug#981404: Fix seems incomplete
Date: Thu, 11 Feb 2021 16:54:53 +0100

Hi Feri,,

On Thu, Feb 11, 2021 at 11:26:47AM +0100, wferi@niif.hu wrote:

> Hi,
>
> The patch in this bug report very much shrinks the window of the vulnerability, but doesn't close it completely: the file is still created with default permissions, then chmodded as a separate step. It's hard, but not impossible to still win the race and open the file before the chmod, enabling the same attack. I recommend something like
>
> ```
> fd = open(dstFileName, O_WRONLY|O_CREAT|O_EXCL, 0600);
> if (fd != -1)
>     f = fdopen( fd, "wb" );
> if (fd == -1 || f == NULL)
>     DISPLAYLEVEL(1, "zstd: %s: %s\n", dstFileName, strerror(errno));
> return f;
> ```
>
> for example.

See #982519 respectively https://github.com/facebook/zstd/issues/2491 upstream.

Regards,

Salvatore

Marked as found in versions libzstd/1.1.2-1. Request was from Étienne Mollier <etienne.mollier@mailoo.org> to control@bugs.debian.org. (Sat, 20 Feb 2021 08:54:02 GMT) (**full text**, **mbox**, **link**).

Bug archived. Request was from Debbugs Internal Request <owner@bugs.debian.org> to internal_control@bugs.debian.org. (Sun, 28 Mar 2021 07:25:05 GMT) (**full text**, **mbox**, **link**).

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

*Debian bug tracking system administrator <**owner@bugs.debian.org**>. Last modified: Fri Dec 16 15:33:50 2022; Machine Name: buxtehude*

Debian Bug tracking system