Das Risiko in der Software-Lieferkette:

Warum Free and Open-Source-Software gefördert werden muss

Christoph Friedrich

Earth Observation Research Cluster / Universität Würzburg

GeoForum des DDGI, 08.11.2024, Berlin

EARTH OBSERVATION RESEARCH

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

FLOSS

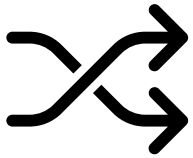
Free *Libre* Open Source Software

Quelloffen. Frei? Kostenlos?

Vorteile von FOSS

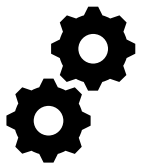
Keine Lizenzkosten

Volle Transparenz



Hohe Flexibilität

Gute Interoperabilität



Keine Abhängigkeit

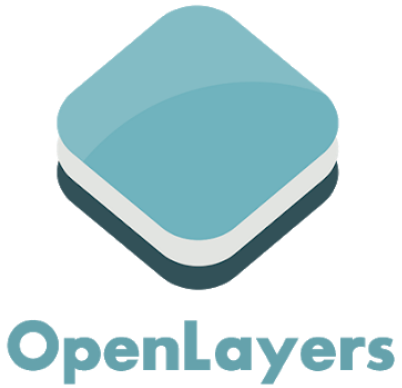
Engagierte Community

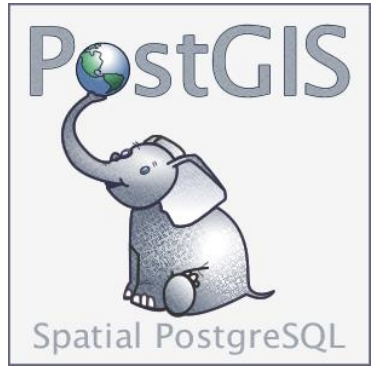
Das Sicherheitsniveau entspricht meist mindestens dem proprietärer Software.

— Myra Security

https://www.myrasecurity.com/de/knowledge-hub/open-source/

FOSS im Geo-Bereich





87,1 %

aller Webseiten nutzen Linux

W3Techs, 2024
https://w3techs.com/technologies/details/os-unix

87,1 %

aller Webseiten nutzen Linux

und höchstwahrscheinlich auch Ihre Organisation

W3Techs, 2024
https://w3techs.com/technologies/details/os-unix

TLP:CLEAR

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lageze

CVSS SCORE
10/10

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

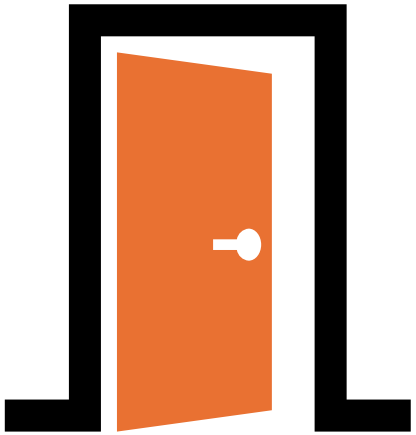
Kritische Backdoor in XZ für Linux

CSW-Nr. 2024-223608-1132, Version 1.1.1, 03.04.2024

IT-Bedrohungslage*: 3 / Orange

Hintertür in XZ Utils

- Hilfsprogramm zur Komprimierung unter Linux
- Ursprünglich von Lasse Collin (seit ca. 2009)
- Seit 2021 Zuarbeiten von „Jia Tan“
- Zunehmend Druck von „weiteren Nutzern“



Re: [xz-devel] XZ for Java

Lasse Collin | Wed, 08 Jun 2022 03:28:08 -0700

On 2022-06-07 Jigar Kumar wrote:
> 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.

I haven't lost interest but my ability to care has been fairly limited
mostly due to longterm mental health issues but also due to some other
things. Recently I've worked off-list a bit with Jia Tan on XZ Utils and
perhaps he will have a bigger role in the future, we'll see.

It's also good to keep in mind that this is an unpaid hobby project.

Anyway, I assure you that I know far too well about the problem that
not much progress has been made. The thought of finding new maintainers
has existed for a long time too as the current situation is obviously
bad and sad for the project.

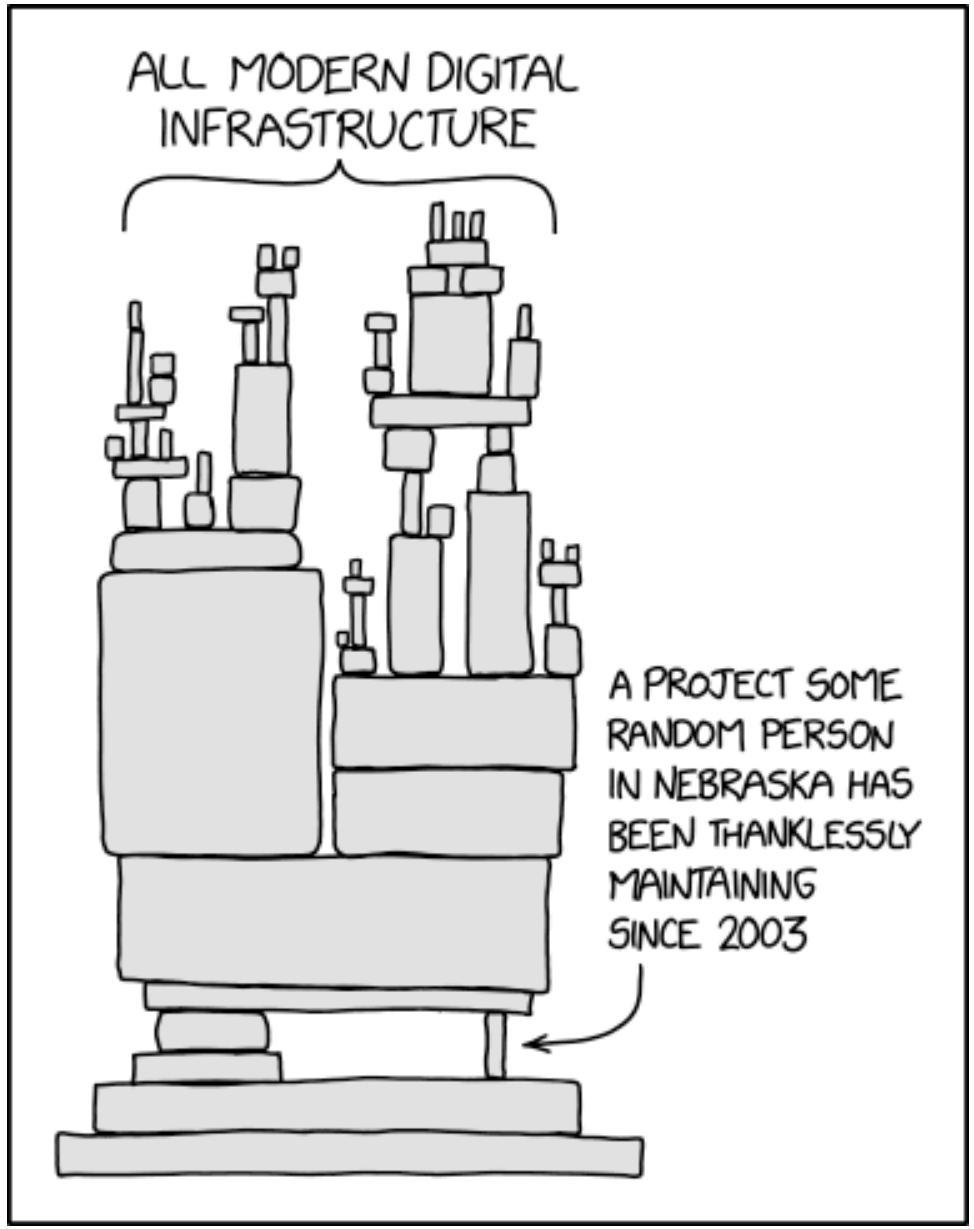
https://www.mail-archive.com/xz-devel@tukaani.org/msg00567.html

Hintertür in XZ Utils

- → „Jia Tan“ bekommt zunehmend Rechte
- Anfang 2024: Getarnte Einschleusung der Hintertür
- Inklusion in Nightly Builds, beinahe in große Releases
- Ende März: Andres Freund entdeckt sie durch großen Zufall

0,8 statt 0,2 sec

THIS IS REAL



Randall Moore: Dependency (2020)
https://www.xkcd.com/2347/

Entwicklung und Wartung von FOSS…

haben große Vorteile für Sie.

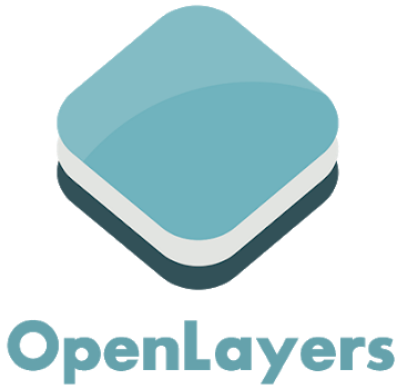
Entwicklung und Wartung von FOSS…

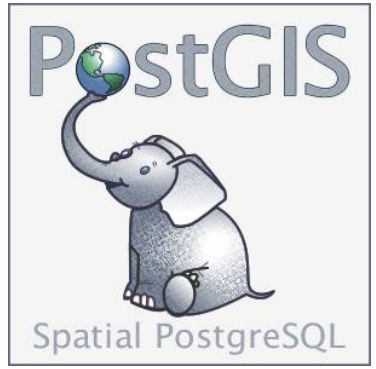
haben große Vorteile für Sie.

kosten Zeit und damit irgendwo Geld.


12. DEUTSCHES GEOFORUM 2024
RISIKEN – VERANTWORTUNG – SICHERHEIT
07.–08.11.2024

FOSS im Geo-Bereich





Software fällt nicht vom Himmel.

Bitte unterstützen Sie die Entwicklung und langfristige Wartung von FOSS-Projekten.

Vielen Dank für Ihre Aufmerksamkeit!

Christoph Friedrich
christoph.friedrich@uni-wuerzburg.de
http://cfriedrich.de/

FOSS4G BELÉM,2024