.Deb

銀河系唯一のDebian専門誌

2024 年 4 月 20 日

xz-utils

デビアン勉強会

目次

1 最近の Debian 関連のミーティング報告

杉本 典充

1.1 2024 年 2 月度 東京エリア・関西合同 Debian 勉強会

2024 年 2 月 17 日 (土) に東京エリア Debian 勉強会と関西 Debian 勉強会の合同でオンラインによる Debian 勉強会を開催しました。参加者は 10 名でした。

セミナー発表は、野首 さんによる「RAG と LLM そして DebGPT」を行いました。

勉強会の終了後、参加者同士で Debian や OSS に関する話の情報交換を行いました。

1.2 OSC 2024 Online/Spring

2024 年 3 月 2 日 (土) に OSC 2024 Online/Spring[*1]が開催されました。イベントの会場は、オンラインの Zoom & YouTube Live でした。

日本 UNIX ユーザ会のセミナーの「IT コミュニティの運営を考える」のパネルディスカッションに東京エリア Debian 勉強会から杉本さんが参加しました。

セミナーの動画は以下 URL で公開しています。

- https://www.youtube.com/watch?v=nMOkv2XPSC8

1.3 OSC 2024 Online/Spring (2024 年 3 月度 東京エリア・関西合同 Debian 勉強会)

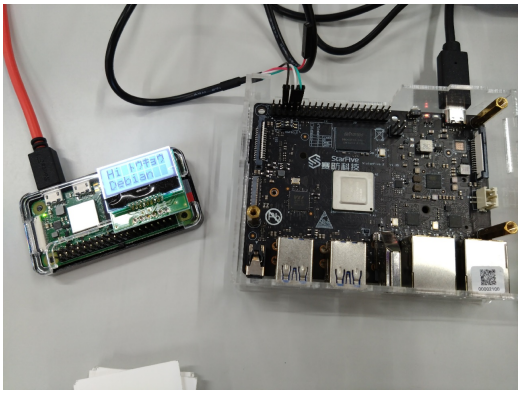
2023 年 3 月 10 日 (日) に Debian JP Project ／東京エリア Debian 勉強会は、オープンソースカンファレンス 2024 Tokyo/Spring[*2]に参加しました。イベントの会場は東京都立産業貿易センター台東館で、イベント全体の参加者は 530 名でした。

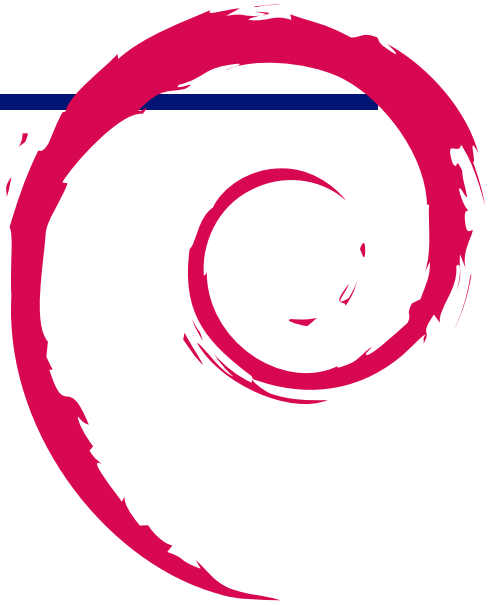
イベントスペースにブースを出展して RISC-V64 のボード PC を展示し、48 名がブースに訪れました。

イベント報告は以下 URL で公開しています。

- https://tokyodebian-team.pages.debian.net/2024-03-osc_report.txt

[*1] https://event.ospn.jp/osc2024-online-spring/
[*2] https://event.ospn.jp/osc2024-spring/


Debian JP Project
Debian

Hi from Debian



2 事前課題

杉本 典充

今回の事前課題は以下です。

1. ファイルの圧縮でよく使う形式を教えてください
2. Debian または他の OS で 32bit 版を使っている場合はその CPU アーキテクチャを教えてください

2.1 dictoss

1. zip, gzip (gz)
2. i386 (x86), arm / armel /armhf

2.2 NOKUBI Takatsugu (knok)

1. zip, gzip (gz)
2. i386 (x86), arm / armel /armhf

2.3 Kazuhiro NISHIYAMA (znz)

1. zip, xz
2. 32bit 版 OS は使っていない

2.4 su_do

1. zip, その他
2. i386 (x86)

2.5 kenhys

1. gzip (gz), xz
2. arm / armel /armhf

2.6 yy_y_ja_jp

1. gzip (gz)
2. i386 (x86)

2.7 sanadan

1. zip
2. 32bit 版 OS は使っていない

2.8 YukiharuYABUKI

1. (回答なし)
2. 32bit 版 OS は使っていない

2.9 hamzootopia

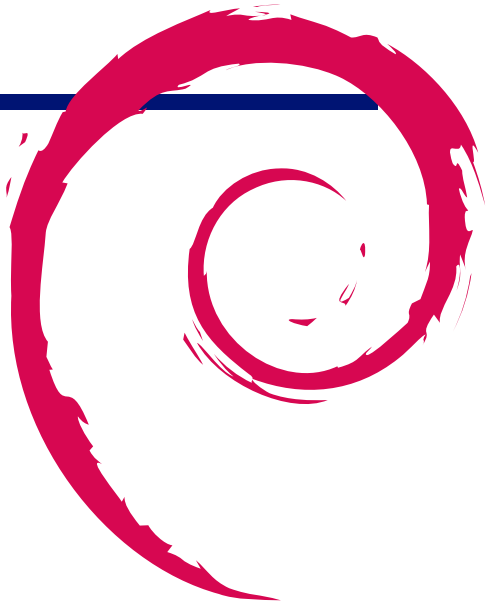
1. (回答なし)
2. (回答なし)

2.10 hihitani

1. zip, lzh, gzip (gz)
2. i386 (x86)

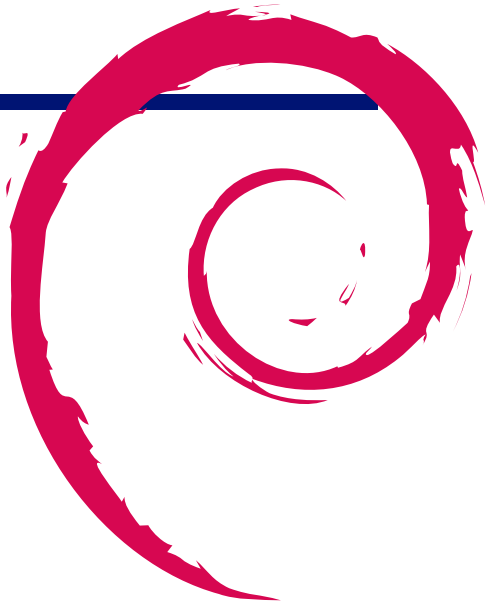
2.11 yukiyam99999999999999999999

1. (回答なし)
2. (回答なし)



3 Debian における 64bit time_t 移行について

林健太郎 (kenhys)



4 xz-utils のバックドア問題の情報交換

2024 年 4 月の参加者

4.1 参加者

参加者は以下の 8 名でした。（敬称略）

- dictoss
- kenhys
- knok
- su_do
- yy_y_ja_jp
- znz
- sanadan
- YukiharuYABUKI

4.2 参考情報

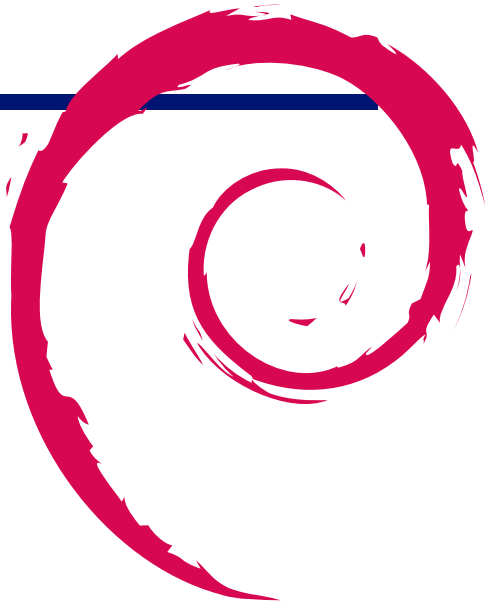
- XZ Utils に悪意のあるコードが挿入された問題（CVE-2024-3094）について
  - https://www.jpcert.or.jp/newsflash/2024040101.html
  - Debian の情報
    - https://security-tracker.debian.org/tracker/CVE-2024-3094
    - https://lists.debian.org/debian-security-announce/2024/msg00057.html
- xz-utils パッケージ (Debian Package Tracking)
  - https://packages.qa.debian.org/x/xz-utils.html
  - 2024-04-20 現在 (stable は bookworm)
    - stable 5.4.1-0.2 (影響なし)
    - testing 5.6.1+really5.4.5-1 (影響あり、バージョンを巻き戻し)
    - unstable 5.6.1+really5.4.5-1 (影響あり、バージョンを巻き戻し)
    - Ubuntu 5.6.1+really5.4.5-1 (影響あり、バージョンを巻き戻し)
- 開発中の Ubuntu 24.04 LTS にも影響があり、ベータ版のリリースが 1 週間遅れた
  - https://gihyo.jp/admin/clip/01/ubuntu-topics/202404/05
- xz backdoor (2024-03-29)
  - https://lists.debian.org/debian-devel/2024/03/msg00333.html
  - 2024-02-28 に unstable で really5.4.5 へ巻き戻し

    * https://tracker.debian.org/news/1515519/
      accepted-xz-utils-561really545-1-source-into-unstable/
- XZ Utils にバックドア攻撃が行われるまでのタイムラインまとめ (2024-04-03 の記事)
  - https://gigazine.net/news/20240403-timeline-of-xz-open-source-attack/
  - Debian unstable に問題のバージョンが混入したのは、2024-02-26
    * 混入直前:https://snapshot.debian.org/archive/debian/20240225T151757Z/pool/main/x/xz-utils/
    * 5.6.0 混入直後:https://snapshot.debian.org/archive/debian/20240226T213049Z/pool/main/x/xz-utils/
    * really 版リリース直後:https://snapshot.debian.org/archive/debian/20240328T211728Z/pool/main/x/xz-utils/
- 分析
  - https://research.swtch.com/xz-script 仕込まれたスクリプトの解析
  - https://boehs.org/node/everything-i-know-about-the-xz-backdoor
    * JiaT75 が xz 以前にも bsdtar に悪意あるコードを PR していた

4.3 参加者の意見

- どういう脆弱性だったのか？
  - xz-utils ライブラリのパッケージが脆弱性を生み出しているが、このコードは ssh のログイン認証を迂回するような細工を行うものだった
  - 問題となったコードは m4 マクロだった
    * 読める人はあまりいない気がする
- debian.org の unstable で今回戻したバージョンは、疑いがある人のコミットが 1 つもないところまで戻している
  - このメンテナーは信用できるのか？という感じで見られている
  - https://joeyh.name/blog/entry/reflections_on_distrusting_xz/
    * joeyh さんがそうすべきとした理由
- debian のバグレポートでもソーシャルハッキングのような感じで、バグ入りのバージョンを入れてほしいと圧力がかかっていた
  - https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1067708
  - debian も攻撃されたと言えると思う
- MiniDebConf ベルリンでこの脆弱性の話の枠がある模様
  - https://salsa.debian.org/ftp-team/xz-2024-incident/-/issues/12
- 今回の問題は人とコードの問題をわけて議論する必要があると思う
- 人の話
  - コミット権はどのような理由で誰に与えるかの問題
    * コミット権の与え方がゆるい人を作らない、というのはいいがその見極めは難しい気がする
    * debian では公的機関が発行した証明書で本人認証をした上で Debian Developer を任命することにしている
  - ソーシャルハッキング
    * 事前に対応するのは難しい
    * 事後対応になりそうなため、どのように対処するか事前にある程度決めておく
- コードの話
  - 今回は tarball にマルウェアのコードが入り込んだが、git にはマルウェアのコードはなかった

    * debian.org では tarball と git の中身をクロスチェックするツールをつくってはどうかという意見あり
- Chain of Responsibility という考え方
- コードを作る人 (upstream) と送り届ける人 (distributor) に分けて考えたほうがいい
    * debian は distributor
- コードのレビューで対応する案もあるが、この対応をボランティアでやりきるのはかなり辛い
    * 実際見抜けるのか、という問題もありそう
- 今回の脆弱性は m4 マクロで埋め込んだものであるが、これは技術的に古く面倒見れる人が少ない
    * autoconf、automake はビルドシステム職人が行う領域な気がする
    * 新しいビルドシステム形式に置き換えを進めるのがいいのか？
    * 辛くないビルドシステムとは何？
        · なにかあるかと言われると困る。どれも辛い気がする
        · スクリプト言語などのビルドしないソースコードが主流になればよい未来が来る？
    * 標準技術は時代とともに変わる
        · `https://www.explainxkcd.com/wiki/index.php/927:_Standards`
- 多様な環境を提供するのが Debian のアイデンティティだと思う
- 対応は個人でできるレベルを超えているため、組織的に関与していかないと対応は難しいと思う



5 メモ

Debian 勉強会資料

2024 年 4 月 20 日　　初版第 1 刷発行

東京エリア Debian 勉強会 （編集・印刷・発行）