ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

## ●圧縮ツール「XZ Utils」に不正なコード埋め込み、サーバーにバックドアの恐れ

https://forest.watch.impress.co.jp/docs/news/1580604.html
https://tukaani.org/xz-backdoor/
https://piyolog.hatenadiary.jp/entry/2024/04/01/035321

### このニュースをザックリ言うと･･･

- 3月29日(現地時間)、圧縮ツール「XZ Utils」の開発元より、XZ Utilsに悪意のあるコードが仕込まれた状態でリリースされていたと発表されました。

- 問題が確認されたのはXZ Utilsバージョン5.6.0/5.6.1で、これらのバージョンがインストールされていた場合、サーバーのsshdにバックドアが仕掛けられ、外部から不正に侵入される恐れがあるとされています。

- この問題は脆弱性「CVE-2024-3094」として扱われ、JPCERT/CC等各セキュリティ団体、XZ Utilsが主に使用されるLinuxの各ディストリビューションおよびmacOSのHomebrewプロジェクト等で注意喚起が出されています。

### AUS便りからの所感等

- 主なLinuxディストリビューション(RHEL派生のCentOS 7・Rocky Linux・Almalinux、あるいはDebian・Ubuntu、等)の安定版で提供されるXZ Utilsのパッケージは、不正なコードが仕込まれる前のバージョン(5.4.5以前)を使用しており、影響を受けないとのことです。

- ただし、前述したディストリビューションでも開発版(Fedora・Rawhide、あるいはDebian testing・unstable)の場合には、一時的にバージョン5.6.0/5.6.1が入り、不正なコードの影響を受ける可能性があったとされています(現在は前のバージョンにダウングレードする等の対策が行われています)。

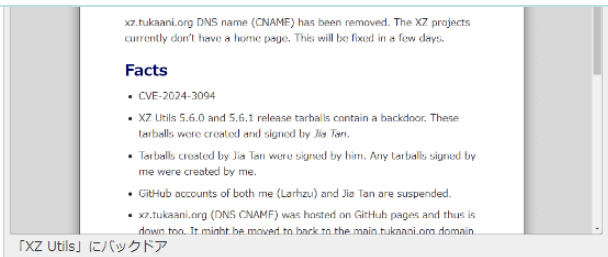
- XZ Utilsの開発に2021年から参加した開発者の一人が、テスト用ファイルに偽装する等して悪意のあるコードを巧妙に仕掛けた「サプライチェーン攻撃」の一種とされており、Microsoftに在籍する開発者がサーバーで発生した不審な挙動等からたまたま問題を発見したとのことです。

- 発見が遅れていたら、安定版においても問題のあるバージョンが採用されていた恐れがあったとされており、不正なコードがOS上にどんな影響を及ぼしていたかについて今後も分析が進められること等が考えられ、引き続き動向が注目されるところです。

**「XZ Utils」にバックドア、オープンソースエコシステム全体の信頼を揺るがす事態に**

0.5秒の遅延からたまたま発覚、数年をかけた周到なやり口が明るみに

樽井 秀人　2024年4月1日 10:16



「XZ Utils」にバックドア

Linux環境で広く利用されているツール「XZ Utils」に3月29日、バックドアが発見されたとのこと（CVE-2024-3094）。Red Hatが評価した「CVSS 3」のベーススコアは、「10.0」（Critical）。長い時間をかけてプロジェクトオーナーの信頼を勝ち取り、メンテナンスを任された開発者が意図的に混入させたという悪質性や、当該ツールが複数の主要なLinuxディストリビューションで採用されており、「OpenSSH」をはじめ影響が広範囲に及ぶ点などが話題を呼び、オープンソースソフトウェアのサプライチェーンのあり方が問われる事態となっている。

## ●ユーザー個人情報・身分証明書・履歴書等約16万人分、外部から閲覧可能な状態だった

https://www.itmedia.co.jp/news/articles/2404/01/news081.html
https://workstyletech.com/incident_report03292024/

### このニュースをザックリ言うと・・・

- 3月29日(日本時間)、ワークスタイルテック社より、同社の労務管理クラウドサービス「WelcomeHR」利用者の個人情報が外部から閲覧可能な状態にあったこと等が発表されました。

- 閲覧可能な状態とされていたのは、当該サービスユーザー162,830人分の氏名・性別・住所・電話番号、ユーザーがアップロードした身分証明書画像(マイナンバーカード・運転免許証等)および履歴書等の画像です。

- うち154,650人分については、第三者によってダウンロードされた形跡が確認されたとしています。

### AUS便りからの所感

- 3月22日に実施されたセキュリティ調査により、2020年1月5日以降サーバーのアクセス権限設定の誤りで閲覧可能状態にあったこと、2023年12月28日～29日にダウンロードが発生していたことが発覚したとのことです。

- 個人情報のみならずマイナカード等の画像と、極めてセンシティブな情報が流出しており、現時点で二次被害は確認されていないとするものの、なりすまし・詐欺行為への悪用が懸念されます。

- 今や企業のシステムや機密情報の保持等においてもクラウドの利用は一般的なものとなっており、クラウドであっても(企業ネットワーク内でサーバーを運営する)オンプレミスであっても、それぞれに必要なアクセス管理設定を確実に行うこと、不要となった機密情報については速やかに破棄すること、これらの設定や情報管理・破棄体制について診断や監査を受けることが重要です。

ITmedia NEWS

**第三者が個人情報15万人分ダウンロード　労務管理クラウド「WelcomeHR」で漏えい　マイナカードや免許証の画像も**

2024年04月01日 11時09分 公開　[ITmedia]

カオナビ子会社のワークスタイルテック（東京都港区）は3月29日、同社の労務管理クラウドサービス「WelcomeHR」について、ユーザー情報が外部から閲覧可能な状態になっていたと発表した。16万2830人分の情報が閲覧可能だったとしており、うち15万4650人分の情報が実際に第三者にダウンロードされたという。

2020年1月5日から24年3月22日にかけて、ユーザーの氏名、性別、住所、電話番号、ユーザーがアップロードした身分証明書（マイナンバーカード、運転免許証、パスポートなど）や履歴書の画像が閲覧可能だった。情報がダウンロードされたのは23年12月28日から29日にかけてだったという。3月29日時点では二次被害は確認していないとしている。

## ●3月はWordPressの27のプラグインに脆弱性…Sucuri社発表

https://blog.sucuri.net/2024/03/wordpress-vulnerability-patch-roundup-march-2024.html
https://wpmake.jp/contents/knowledge/202403wp-news/

### このニュースをザックリ言うと・・・

- 3月25日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、3月に報告された27のWordPressプラグインに存在する30件の脆弱性のまとめ記事が発表されました。

- 今回発表分は全てクロスサイトスクリプティング(XSS)の脆弱性となっています。

- うち、最も危険度が高い「High」にあたるのは「Essential Addons for Elementor」「WP Statistics」で発見された2件となります。

### AUS便りからの所感

- WordPressにおいては、提供されるプラグインも、またそれらで報告される脆弱性も数多く存在しており、Sucuri社による月毎のまとめでは、1月分で28件、2月分で29件と、多数の報告がまとめられています(ただし別の情報源ではここでまとめられていない脆弱性も報告されており、調査の際は複数の情報源をあたることが重要です)。

- WordPress本体においても1月にセキュリティアップデート6.4.3がリリースされるなど、不定期に更新されることがあり、本体・プラグインともインストールした状態のままで放置するようなことは決してせず最新に保つよう努めること、加えてセキュリティを強化する何らかのプラグインを導入し、さらに並行して(もしくは本体・プラグインのアップデートが困難な場合を鑑みて)WAFやIDS・IPSの導入についても検討するのが良いでしょう。

SUCURI

**WordPress Vulnerability & Patch Roundup March 2024**

SUCURI MALWARE RESEARCH TEAM
March 25, 2024

Vulnerability reports and responsible disclosures are essential for website security awareness and education. Automated attacks targeting known software vulnerabilities are one of the leading causes of website compromises.

To help educate website owners about potential threats to their environments, we've compiled a list of important security updates and vulnerability patches for the WordPress ecosystem this past month.

The vulnerabilities listed below are virtually patched by the Sucuri Firewall and existing clients are protected. If you don't have it installed yet, you can use our web application firewall to protect your site against known vulnerabilities.