INTELLILINK セキュリティ情報配信サービス
注目されているセキュリティ事故・事件に関する情報
＜2022年3月版 (第40号)＞ (選り抜き版)

2022年3月29日
ＮＴＴデータ先端技術株式会社
セキュリティ事業本部

今回のサマリー

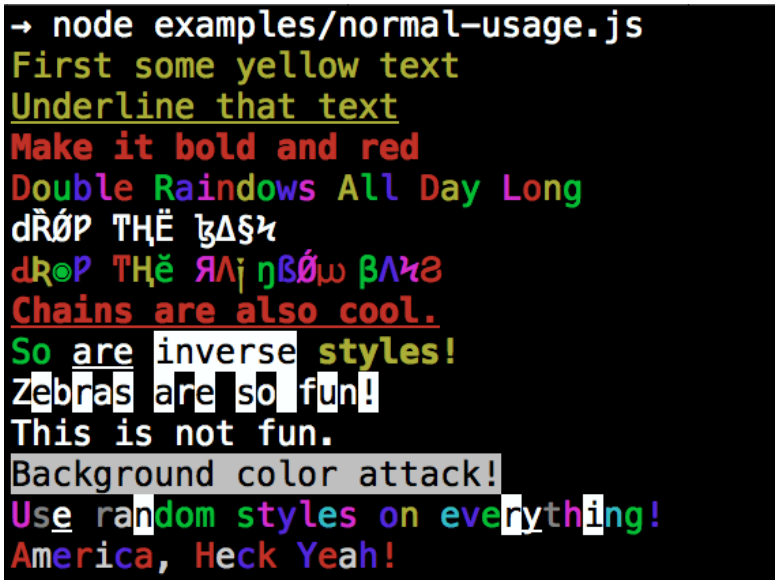
OSS開発者による意図的な改変
人気のオープンソースのライブラリである「colors.js」と「faker.js」の開発者が、企業からの資金提供がないことを理由に機能しなくなる改変をする事案がありました。多くのOSSがこれらのライブラリを使用しており、OSSサプライチェーンの汚染事案として大きな影響がありました。本記事では、OSSを利用する組織がとるべき対策について解説します。

OSS開発者による意図的な改変

1. 事案概要

2022年1月8月、node.js向けのnpmパッケージである「colors.js」と「faker.js」が、開発者によって機能しなくなるコードに改変されました。開発者は改変の理由を、1年以上企業に求めてきた金銭的サポートがなかったためとしています。

「colors.js」はコンソールの色を変えるライブラリで、約19,000件のnpmパッケージが依存しています。「faker.js」はダミーデータを作成するライブラリで、約2,500件のnpmパッケージが依存しています。



colors.jsのデモ。コンソールの文字を色付けできる。
出典：https://www.npmjs.com/package/colors

改変の影響を受けたAWS Cloud Development Kitのバグ報告。
コンソールの表示が乱れている。
出典：https://github.com/aws/aws-cdk/issues/18322

2. 影響を受けるバージョン

開発者の改変によって影響を受けるバージョンは以下の通りです。現在、これらのバージョンはリポジトリから削除されており、問題のないバージョンまでロールバックされています。

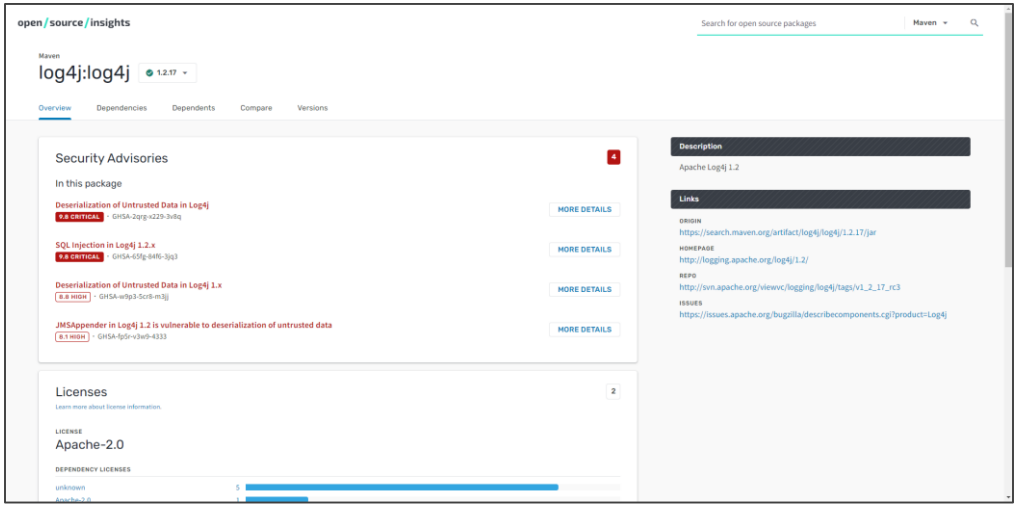
プロダクト名	影響を受けるバージョン	修正された(ロールバックされた)バージョン
colors.js	1.4.44-liberty-2	1.4.0
	1.4.1	
	1.4.2	
faker.js	6.6.6	5.5.3

3. 対策 「システムで利用しているOSSの把握」

本件は、OSS利用者から見るとサプライチェーンが汚染された事案です。これはOSSにバックドアやマルウェアが混入した状況と類似しているため、同様の対策が有効です。

今日のITシステムはOSSに多くを依存しており、**ソフトウェアサプライチェーンの汚染リスクを回避することは極めて困難**なため、影響を最小限にする対策を行うことが重要です。

対策の前の準備として、**現在使用しているOSSを把握する**ことが必要です。例えば、Googleによる「Open Source Insights」は、OSSの依存関係を容易に確認することができます。



例：Apache Log4jにおける依存関係。Open Source Insightsでは依存元と先のプロダクトだけでなくセキュリティアドバイザリやライセンスも確認できる。
出典：https://deps.dev/maven/log4j%3Alog4j/

4. 対策 「システムの開発・導入の各工程でのリスクの考慮」

システムの開発や導入においては、その**要件定義・設計・運用の各フェーズで、リスクを軽減し、影響を最小限にする**ための対策が重要です。

一般的にソフトウェアを導入する際には、システムの機能性や信頼性を維持するために提供する企業によるサポート体制や脆弱性対応などの確認が必要ですが、**OSSの場合はサポートはないものとして扱う必要があります**※。OSSはライセンスの下で利用することができますが、ライセンスには利用者の責任において利用する条項が明記されていることがほとんどです。これは開発者が「colors.js」に適用しているMITライセンスにおいても同様です。

> 作者または著作権者は、契約行為、不法行為、またはそれ以外であろうと、ソフトウェアに起因または関連し、あるいはソフトウェアの使用またはその他の扱いによって生じる一切の請求、損害、その他の義務について何らの責任も負わないものとします。

MITライセンスの日本語訳(一部抜粋) 出典：https://licenses.opensource.jp/MIT/MIT.html

そのため、要件定義・設計時には、問題が発生した際に問題のない状態のバックアップへの切り戻しや、代替となるOSSが使用できるように考慮する必要があります。またはOSSをフォークすることで、OSS開発者として独自に改良することも考えられます。

また、運用時には、定期的なセキュリティ情報の収集とシステムの評価を実施し、問題発生時に備えた対応体制の整備が必要です。

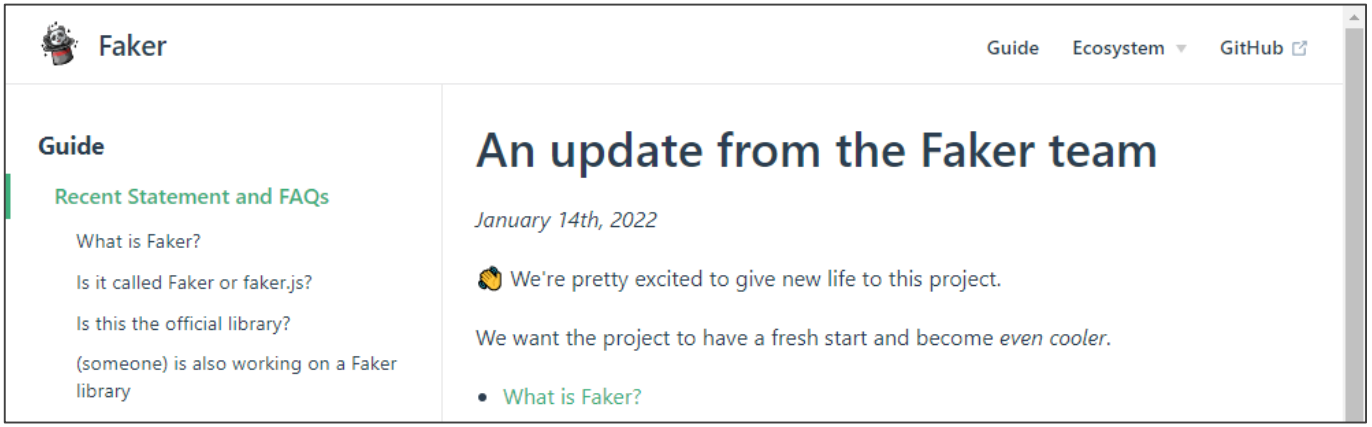
(※) 特定のOSSに対するサポートサービスを提供する企業もあります。

5. 対策 「OSSプロジェクトと開発者へのサポート」

本件で開発者が機能しなくなるコードに改変した根本の原因は、OSS開発者に対してそれを利用する企業からの資金提供などのサポートがなかったためです。OSSを利用するのみのユーザは開発に貢献しない「フリーライダー」と呼ばれ、OSS開発者からは敬遠されます。

OSS開発者へのサポートは開発者への資金や開発環境の提供など大規模ものから、バグの報告やバグを修正するパッチの提供など小規模でも重要なものまで様々です。

なお、本件によって、2022年1月14日にfaker.jsはOpen Source Collectiveの資金援助によって、開発者個人ではなく複数人のメンテナによるコミュニティ主導のプロジェクトとなりました。



faker.jsの開発体制刷新を知らせる記事 出典：https://fakerjs.dev/update.html

6. まとめ

人気のOSSライブラリが開発者によって機能しないものに改変されました。原因はOSSを利用する企業からのサポートがなかったことにあります。OSSを利用するのみのユーザは開発に貢献しない「フリーライダー」と呼ばれ、OSS開発者からは敬遠されます。

OSSはライセンスの下で利用することができますが、その特性上サポートはないものとして扱う必要があります。本件のようなケースに備えて、OSSを利用してシステムやアプリケーションを開発・運用している組織はサプライチェーンの汚染リスクを考慮した対策が必要です。

更に、本件のような事態を引き起こさないためにも、組織は利用しているOSSへのなんらかの貢献をすることが必要となってきます。OSSへのサポートは単なる資金提供だけでなく、バグの報告やパッチの提供も有効です。

組織は適用されたライセンスの下でOSSを利用することができますが、その成果を享受する対価として、OSS開発者が持続的に開発できるように積極的にサポートすることが、利用しているシステムの機能性や信頼性の維持につながります。

7. 参考URL

- colors.js
  https://github.com/Marak/colors.js
- faker.js (現在は削除されている)
  https://github.com/Marak/faker.js
- Open Source Insights
  https://deps.dev/
- An update from the Faker team | Faker
  https://fakerjs.dev/update.html

NTT DATA

Trusted Global Innovator