

On the Impact of Outdated and Vulnerable Javascript Packages in Docker Images

Ahmed Zerouali, Valerio Cosentino, Gregorio Robels, Jesus M. Gonzalez-Barahona

Proceedings of the 2019 IEEE 26th International Conference on
Software Analysis, Evolution and Reengineering (SANER) pages 619–623

発表者：辻 裕真

背景

- Dockerイメージにはnpm (JavaScript), PyPI (Python), CRAN (R)などの一般的なパッケージマネージャーから多くのパッケージがインストールされている.
- それらのパッケージには古いものも多く含まれており, バグやセキュリティの脆弱性の影響を受ける可能性がある.
- Dockerイメージに含まれるnpmパッケージの中で古いものや脆弱性のあるものを調べそれらが与える影響を調査する.

Research Questions

RQ1 : 公式Dockerイメージで使用されているnpmパッケージはどのくらい古くなっているか.

RQ2 : 公式Dockerイメージのnpmパッケージはどの程度脆弱か.

データセット

- Dockerの124の公式リポジトリ内の全てのイメージ（8,891）からnodeを使用している961のイメージを抽出.
- npmからパッケージをインストールする際に作成されるファイル“package.json”からインストールされているパッケージを取得.
- Snyk.ioで公開されているnpmパッケージの脆弱性に関する1,099のレポートを収集.

結果：RQ1

更新日での技術的遅れ（日数差）

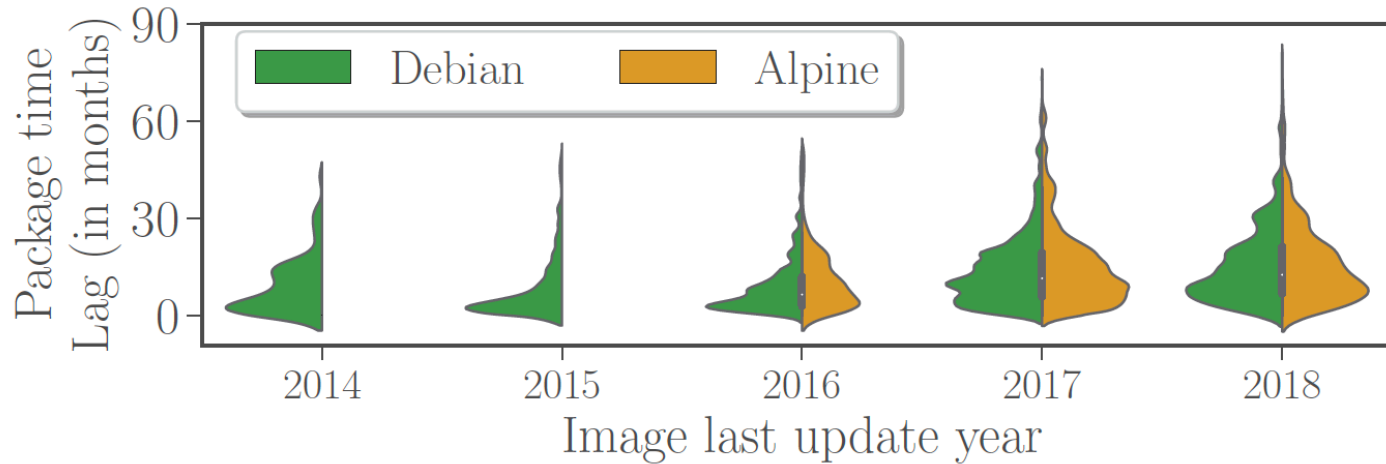


Fig. 1. Yearly distribution of the time lag (calculated at the date of the image's last update) for all outdated packages, grouped by operating system.

利用可能な最新パッケージからの遅れ

最新パッケージの割合

Debian : 64%

Alpine : 57%

結果：RQ1

更新日での技術的遅れ（バージョン差）

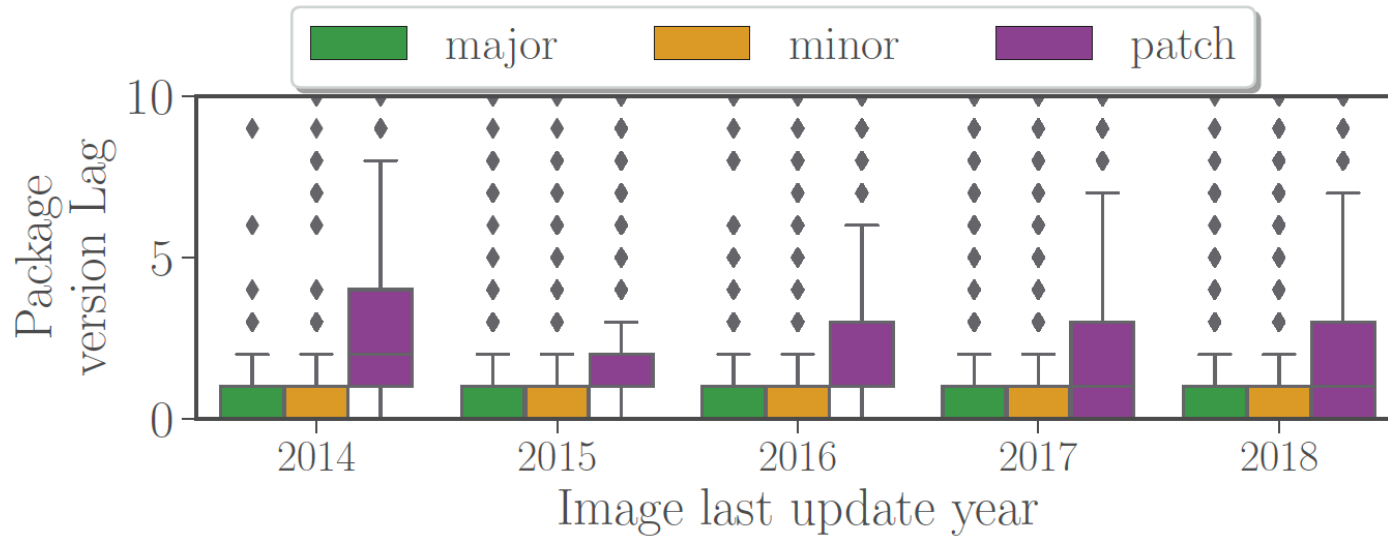


Fig. 2. Yearly distribution of version lag (calculated at the date of image's last update) for all outdated packages in images.

利用可能な最新パッケージからの遅れ

バージョン差の中央値

0 major + 0 minor + 1 patch

結果：RQ1

分析日での技術的遅れ

最新パッケージの割合

Debian : 41%

Alpine : 34%

バージョン差の中央値

2014 : 1 major + 1 minor + 4 patch

2018 : 0 major + 1 minor + 1 patch



Fig. 3. Yearly distribution of version lag (calculated at the date of March 13th 2018) for all outdated packages in images.

古いnodeイメージを使用すると

1つのメジャーアップデートが行われていないパッケージが存在する

結果：RQ2

- 1,099の脆弱性のうちDockerイメージ内のnpmパッケージに影響を与えていたのは74のみであった.
- インストールされている全てのパッケージ（1,412）の内3.7% (52)のパッケージがこの脆弱性の影響を受ける.
- 全てのイメージには何らかの脆弱性が含まれていた.

TABLE II
THE TOP 5 VULNERABILITY TYPES FOUND FOR NPM PACKAGES IN
DOCKER CONTAINERS.

Vulnerability type	% affected containers	# unique affected packages
ReDoS	100	29
Uninitialized Memory Exposure	100	7
Prototype Pollution	100	4
Access Restriction Bypass	100	1
Prototype Override Protection Bypass	79	1

結果：RQ2

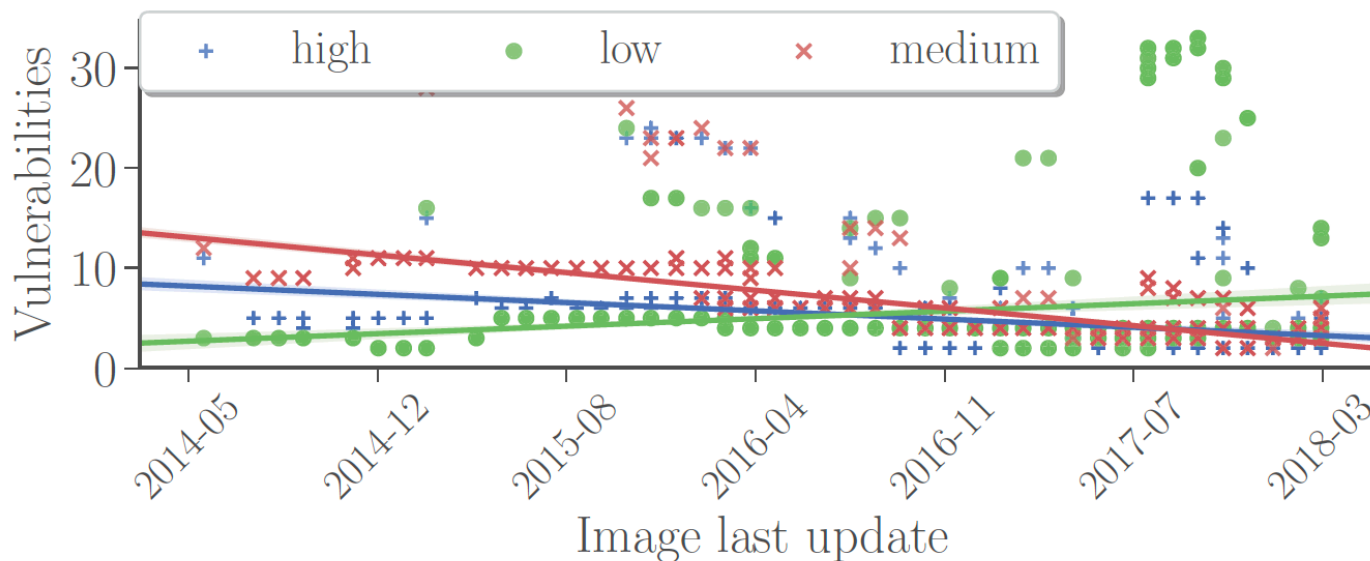


Fig. 4. Image last update and number of vulnerabilities found in it.

イメージの最終更新月ごとの脆弱性の数の分布

古いイメージには脆弱性が多い（弱い脆弱性は除く）

まとめ

- Docker公式イメージ内にインストールされているnpmパッケージの古さ，脆弱性について調査を行った.
- 最新のパッケージがインストールされているイメージが多かったが，全てのイメージには脆弱性のあるパッケージが含まれていた.
- 更新されていないイメージはパッケージも古く脆弱性も多かった.

所感

- ・ コンテナにインストールされているパッケージの特定の仕方が参考になりそう.
- ・ きちんとメンテナンスされている公式イメージだけでの調査なので、他のイメージではかなり結果が変わりそう.