WordCamp US 2023

Ensuring Plugin GPL-compatibility via GitHub Actions

Presented by

Jeff Paul

2023

Jeff Paul

Director of Open Source Initiatives

jeff.paul@10up.com // 10up.com

@jeffpaul

jeffpaul.com

Rainbow Street Art, Reykjavík, Iceland
10up Summit 2023

Introducing 10up's Open Source Practice

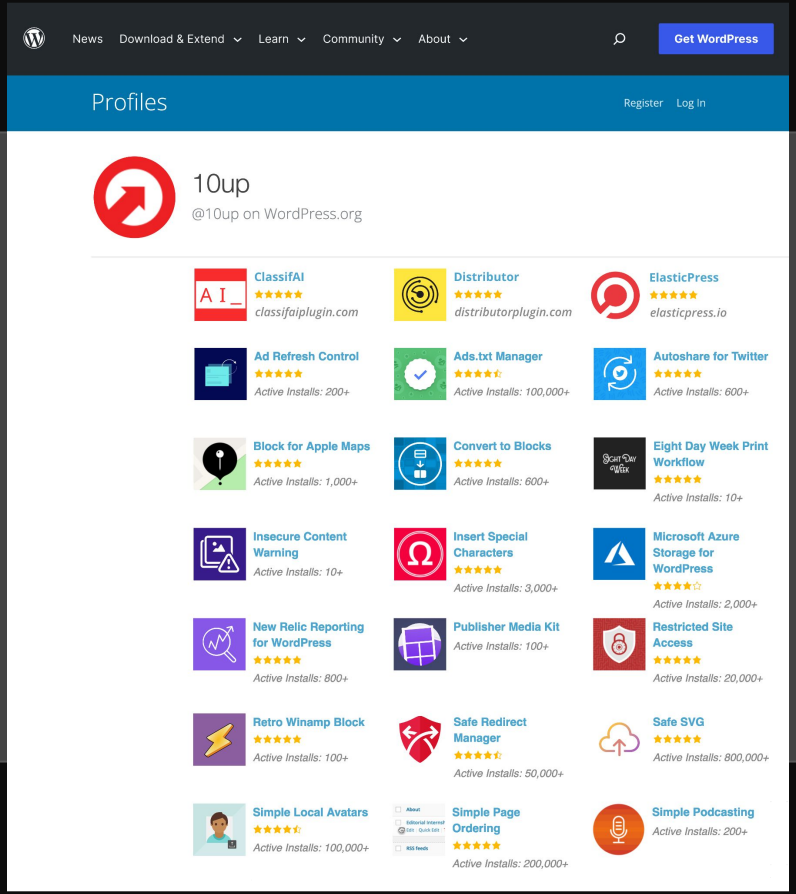
JEFF PAUL on SEPTEMBER 12, 2019

10up aims to make a better web through finely crafted websites, innovative tools for content creators, and open-source contributions that drive growth. As a leading contributor to WordPress and the

Seventeen 10uppers Contribute to WordPress 6.3

JEFF PAUL on AUGUST 25

Earlier this month, WordPress released its 6.3 update, "Lionel", bringing with it significant advancements to the Block Editor, notable performance improvements, and other core updates such as accessibility and internationalization enhancements. **Seventeen 10uppers made contributions to the release,** making a total of 290 contributions to improve the world's most popular CMS.


News
Download & Extend
Learn
Community
About
Get WordPress
Profiles
Register
Log In
10up
@10up on WordPress.org
ClassifAI
classifaiplugin.com
Distributor
distributorplugin.com
ElasticPress
elasticpress.io
Ad Refresh Control
Active Installs: 200+
Ads.txt Manager
Active Installs: 100,000+
Autoshare for Twitter
Active Installs: 600+
Block for Apple Maps
Active Installs: 1,000+
Convert to Blocks
Active Installs: 600+
Eight Day Week Print Workflow
Active Installs: 10+
Insecure Content Warning
Active Installs: 10+
Insert Special Characters
Active Installs: 3,000+
Microsoft Azure Storage for WordPress
Active Installs: 2,000+
New Relic Reporting for WordPress
Active Installs: 800+
Publisher Media Kit
Active Installs: 100+
Restricted Site Access
Active Installs: 20,000+
Retro Winamp Block
Active Installs: 100+
Safe Redirect Manager
Active Installs: 50,000+
Safe SVG
Active Installs: 800,000+
Simple Local Avatars
Active Installs: 100,000+
Simple Page Ordering
Active Installs: 200,000+
Simple Podcasting
Active Installs: 200+

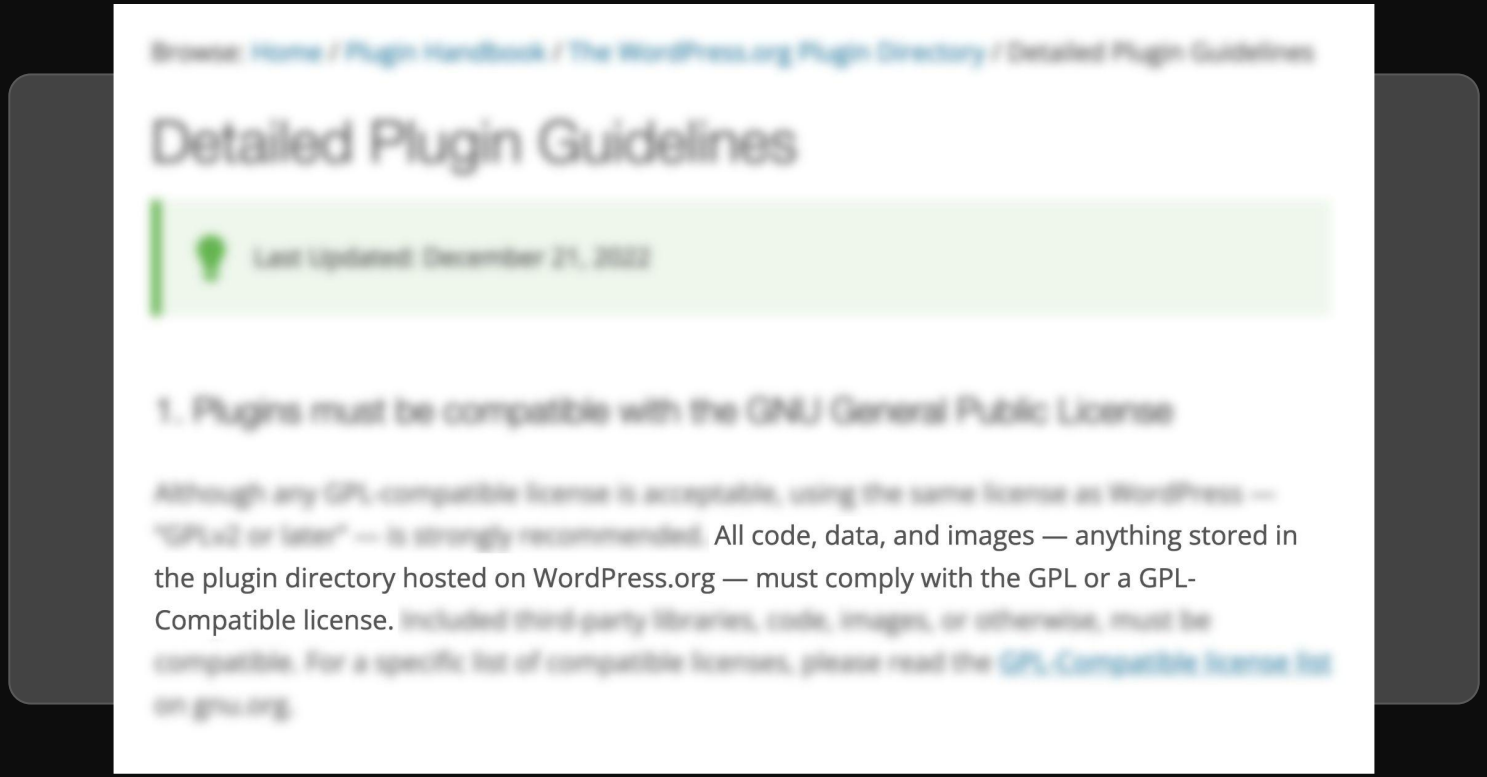
Browse: Home / Plugin Handbook / The WordPress.org Plugin Directory / Detailed Plugin Guidelines

Detailed Plugin Guidelines

Last Updated: December 21, 2022

1. Plugins must be compatible with the GNU General Public License

Although any GPL-compatible license is acceptable, using the same license as WordPress — "GPLv2 or later" — is strongly recommended. All code, data, and images — anything stored in the plugin directory hosted on WordPress.org — must comply with the GPL or a GPL-Compatible license. Included third-party libraries, code, images, or otherwise, must be compatible. For a specific list of compatible licenses, please read the GPL-Compatible license list on gnu.org.



Browse: Home / Plugin Handbook / The WordPress.org Plugin Directory / Detailed Plugin Guidelines

Detailed Plugin Guidelines

Last Updated: December 21, 2022

1. Plugins must be compatible with the GNU General Public License

Although any GPL-compatible license is acceptable, using the same license as WordPress — "GPLv2 or later" — is strongly recommended. All code, data, and images — anything stored in the plugin directory hosted on WordPress.org — must comply with the GPL or a GPL-Compatible license. Included third-party libraries, code, images, or otherwise, must be compatible. For a specific list of compatible licenses, please read the GPL Compatible license list on gnu.org.

Browse: Home / Plugin Handbook / The WordPress.org Plugin Directory / Detailed Plugin Guidelines

Detailed Plugin Guidelines

Last Updated: December 21, 2022

1. Plugins must be compatible with the GNU General Public License

Although any GPL-compatible license is acceptable, using the same license as WordPress — "GPLv2 or later" — is strongly recommended. All code, data, and images — anything stored in the plugin directory hosted on WordPress.org — must comply with the GPL or a GPL-Compatible license. Included third-party libraries, code, images, or otherwise, must be compatible. For a specific list of compatible licenses, please read the GPL Compatible license list on gnu.org.

Licensing Nightmares

What if a PR introduces a new dependency with an incompatible license?

... OR ...

... WAIT ...

... WHAT IF ...

What if we ALREADY have a dependency with an incompatible license?

GitHub Actions to the rescue!

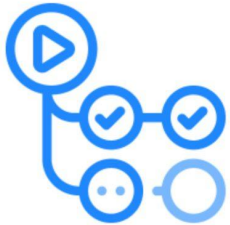
Check new and updated dependencies

Confirm license compatibility

Scan existing codebase

Scan all pull requests

actions/**dependency-review-action**



A GitHub Action for detecting vulnerable dependencies and invalid licenses in your PRs

21 Contributors | 14k Used by | 416 Stars | 102 Forks

github.com

GitHub - actions/dependency-review-action: A GitHub Action for detecting vulnerable dependencies and invalid licenses in your PRs

A GitHub Action for detecting vulnerable dependencies and invalid lic...

Steps to success

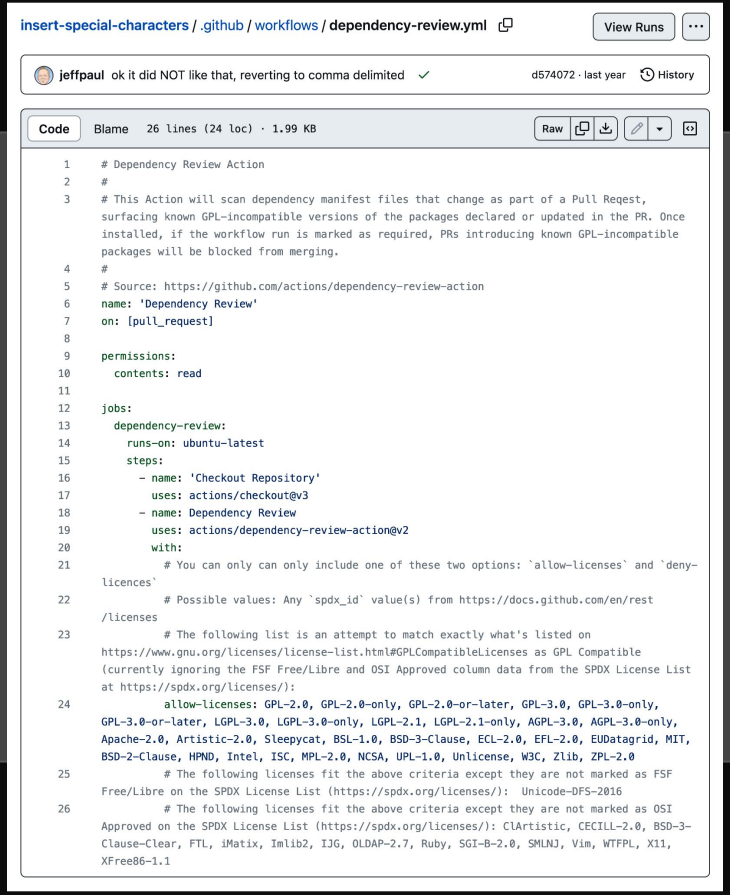
Add Dependency Review Action workflow file

Add GPL-compatible licenses to workflow file

Await results on scan of current codebase

All future PRs checked against license list

Optional: if you maintain multiple plugins, leverage a central license policy file



insert-special-characters / .github / workflows / dependency-review.yml

View Runs

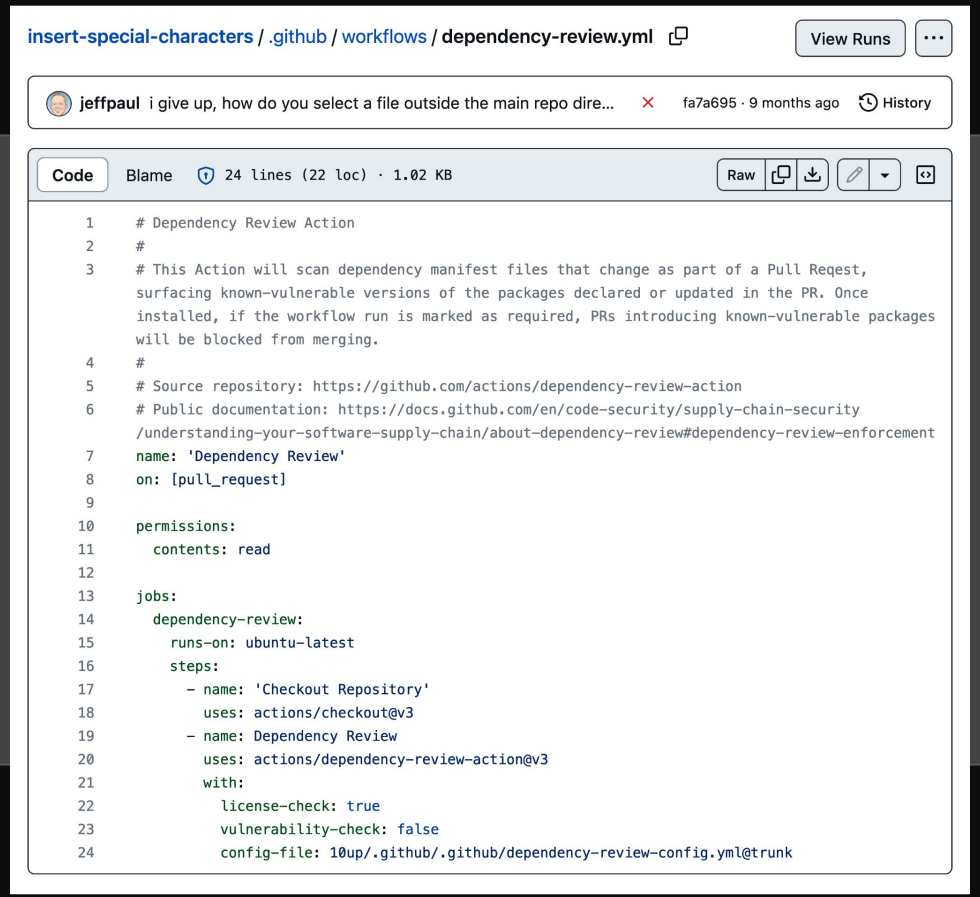
jeffpaul ok it did NOT like that, reverting to comma delimited ✓ d574072 · last year History

Code Blame 26 lines (24 loc) · 1.99 KB Raw

```yaml
# Dependency Review Action
#
# This Action will scan dependency manifest files that change as part of a Pull Reqest, surfacing known GPL-incompatible versions of the packages declared or updated in the PR. Once installed, if the workflow run is marked as required, PRs introducing known GPL-incompatible packages will be blocked from merging.
#
# Source: https://github.com/actions/dependency-review-action
name: 'Dependency Review'
on: [pull_request]

permissions:
  contents: read

jobs:
  dependency-review:
    runs-on: ubuntu-latest
    steps:
      - name: 'Checkout Repository'
        uses: actions/checkout@v3
      - name: Dependency Review
        uses: actions/dependency-review-action@v2
        with:
          # You can only can only include one of these two options: `allow-licenses` and `deny-licences`
          # Possible values: Any `spdx_id` value(s) from https://docs.github.com/en/rest/licenses
          # The following list is an attempt to match exactly what's listed on https://www.gnu.org/licenses/license-list.html#GPLCompatibleLicenses as GPL Compatible (currently ignoring the FSF Free/Libre and OSI Approved column data from the SPDX License List at https://spdx.org/licenses/):
          allow-licenses: GPL-2.0, GPL-2.0-only, GPL-2.0-or-later, GPL-3.0, GPL-3.0-only, GPL-3.0-or-later, LGPL-3.0, LGPL-3.0-only, LGPL-2.1, LGPL-2.1-only, AGPL-3.0, AGPL-3.0-only, Apache-2.0, Artistic-2.0, Sleepycat, BSL-1.0, BSD-3-Clause, ECL-2.0, EFL-2.0, EUDatagrid, MIT, BSD-2-Clause, HPND, Intel, ISC, MPL-2.0, NCSA, UPL-1.0, Unlicense, W3C, Zlib, ZPL-2.0
          # The following licenses fit the above criteria except they are not marked as FSF Free/Libre on the SPDX License List (https://spdx.org/licenses/):  Unicode-DFS-2016
          # The following licenses fit the above criteria except they are not marked as OSI Approved on the SPDX License List (https://spdx.org/licenses/): ClArtistic, CECILL-2.0, BSD-3-Clause-Clear, FTL, iMatix, Imlib2, IJG, OLDAP-2.7, Ruby, SGI-B-2.0, SMLNJ, Vim, WTFPL, X11, XFree86-1.1
```



insert-special-characters / .github / workflows / **dependency-review.yml** View Runs ···

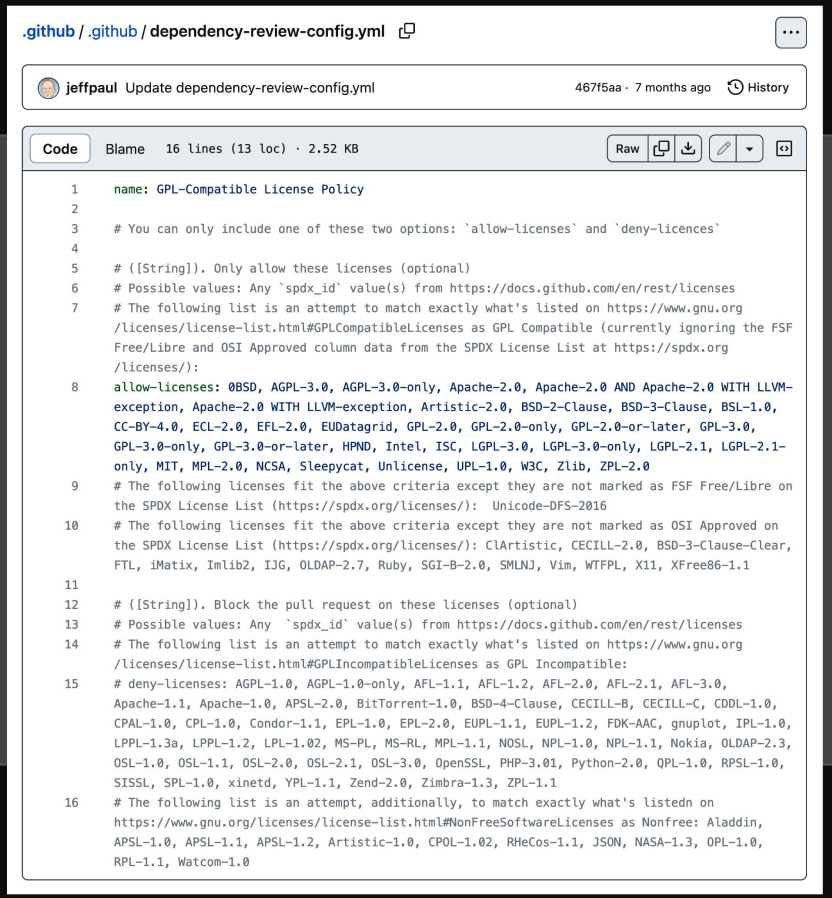
jeffpaul i give up, how do you select a file outside the main repo dire... ✕ fa7a695 · 9 months ago History

Code Blame 24 lines (22 loc) · 1.02 KB Raw

```yaml
# Dependency Review Action
#
# This Action will scan dependency manifest files that change as part of a Pull Reqest,
surfacing known-vulnerable versions of the packages declared or updated in the PR. Once
installed, if the workflow run is marked as required, PRs introducing known-vulnerable packages
will be blocked from merging.
#
# Source repository: https://github.com/actions/dependency-review-action
# Public documentation: https://docs.github.com/en/code-security/supply-chain-security
/understanding-your-software-supply-chain/about-dependency-review#dependency-review-enforcement
name: 'Dependency Review'
on: [pull_request]

permissions:
  contents: read

jobs:
  dependency-review:
    runs-on: ubuntu-latest
    steps:
      - name: 'Checkout Repository'
        uses: actions/checkout@v3
      - name: Dependency Review
        uses: actions/dependency-review-action@v3
        with:
          license-check: true
          vulnerability-check: false
          config-file: 10up/.github/.github/dependency-review-config.yml@trunk
```



.github / .github / dependency-review-config.yml

jeffpaul Update dependency-review-config.yml 467f5aa · 7 months ago History

Code Blame 16 lines (13 loc) · 2.52 KB Raw

```yaml
name: GPL-Compatible License Policy

# You can only include one of these two options: `allow-licenses` and `deny-licences`

# ([String]). Only allow these licenses (optional)
# Possible values: Any `spdx_id` value(s) from https://docs.github.com/en/rest/licenses
# The following list is an attempt to match exactly what's listed on https://www.gnu.org/licenses/license-list.html#GPLCompatibleLicenses as GPL Compatible (currently ignoring the FSF Free/Libre and OSI Approved column data from the SPDX License List at https://spdx.org/licenses/):
allow-licenses: 0BSD, AGPL-3.0, AGPL-3.0-only, Apache-2.0, Apache-2.0 AND Apache-2.0 WITH LLVM-exception, Apache-2.0 WITH LLVM-exception, Artistic-2.0, BSD-2-Clause, BSD-3-Clause, BSL-1.0, CC-BY-4.0, ECL-2.0, EFL-2.0, EUDatagrid, GPL-2.0, GPL-2.0-only, GPL-2.0-or-later, GPL-3.0, GPL-3.0-only, GPL-3.0-or-later, HPND, Intel, ISC, LGPL-3.0, LGPL-3.0-only, LGPL-2.1, LGPL-2.1-only, MIT, MPL-2.0, NCSA, Sleepycat, Unlicense, UPL-1.0, W3C, Zlib, ZPL-2.0
# The following licenses fit the above criteria except they are not marked as FSF Free/Libre on the SPDX License List (https://spdx.org/licenses/):  Unicode-DFS-2016
# The following licenses fit the above criteria except they are not marked as OSI Approved on the SPDX License List (https://spdx.org/licenses/): ClArtistic, CECILL-2.0, BSD-3-Clause-Clear, FTL, iMatix, Imlib2, IJG, OLDAP-2.7, Ruby, SGI-B-2.0, SMLNJ, Vim, WTFPL, X11, XFree86-1.1

# ([String]). Block the pull request on these licenses (optional)
# Possible values: Any  `spdx_id` value(s) from https://docs.github.com/en/rest/licenses
# The following list is an attempt to match exactly what's listed on https://www.gnu.org/licenses/license-list.html#GPLIncompatibleLicenses as GPL Incompatible:
# deny-licenses: AGPL-1.0, AGPL-1.0-only, AFL-1.1, AFL-1.2, AFL-2.0, AFL-2.1, AFL-3.0, Apache-1.1, Apache-1.0, APSL-2.0, BitTorrent-1.0, BSD-4-Clause, CECILL-B, CECILL-C, CDDL-1.0, CPAL-1.0, CPL-1.0, Condor-1.1, EPL-1.0, EPL-2.0, EUPL-1.1, EUPL-1.2, FDK-AAC, gnuplot, IPL-1.0, LPPL-1.3a, LPPL-1.2, LPL-1.02, MS-PL, MS-RL, MPL-1.1, NOSL, NPL-1.0, NPL-1.1, Nokia, OLDAP-2.3, OSL-1.0, OSL-1.1, OSL-2.0, OSL-2.1, OSL-3.0, OpenSSL, PHP-3.01, Python-2.0, QPL-1.0, RPSL-1.0, SISSL, SPL-1.0, xinetd, YPL-1.1, Zend-2.0, Zimbra-1.3, ZPL-1.1
# The following list is an attempt, additionally, to match exactly what's listedn on https://www.gnu.org/licenses/license-list.html#NonFreeSoftwareLicenses as Nonfree: Aladdin, APSL-1.0, APSL-1.1, APSL-1.2, Artistic-1.0, CPOL-1.02, RHeCos-1.1, JSON, NASA-1.3, OPL-1.0, RPL-1.1, Watcom-1.0
```

Scan existing codebase

Determine GPL or GPLv2 compatibility

Nervously await results 🤞

If issues, fix & release updated version

Scan all pull requests

GitHub Action runs on future PRs

Passing check validates dependency licenses

No more licensing nightmares 🎉

WordCamp US 2023

Ensuring Plugin GPL-compatibility via GitHub Actions

Presented by

Jeff Paul

Create GitHub Action

<repo>/.github/workflows/dependency-review.yml

Create License Policy (Optional)

<repo>/.github/.github/dependency-review-config.yml

Check Codebase and PRs

🤞 and 🎉

Questions?

Director of Open Source Initiatives

jeff.paul@10up.com // 10up.com

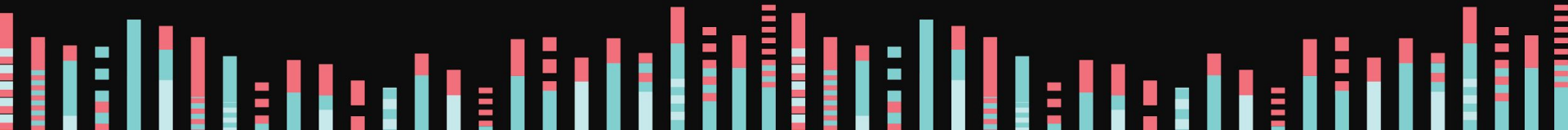
@jeffpaul

jeffpaul.com

WordCamp US 2023

Appendix

Jeff Paul



GeekMasher/**advanced-security-compliance**

GitHub Advance Security Compliance Action

8 Contributors

66 Used by

124 Stars

26 Forks

github.com

GitHub - GeekMasher/advanced-security-compliance: GitHub Advance Security Compliance Action

GitHub Advance Security Compliance Action. Contribute to GeekMashe...

WordPress.org Plugin Directory Guidelines:
https://developer.wordpress.org/plugins/wordpress-org/detailed-plugin-guidelines/#1-plugins-must-be-compatible-with-the-gnu-general-public-license

Dependency Review Action: https://github.com/actions/dependency-review-action

Sample Dependency Review Workflow:
https://github.com/10up/insert-special-characters/blob/develop/.github/workflows/dependency-review.yml

Sample GPL-Compatible License Policy:
https://github.com/10up/.github/blob/trunk/.github/dependency-review-config.yml