Evaluating Safety

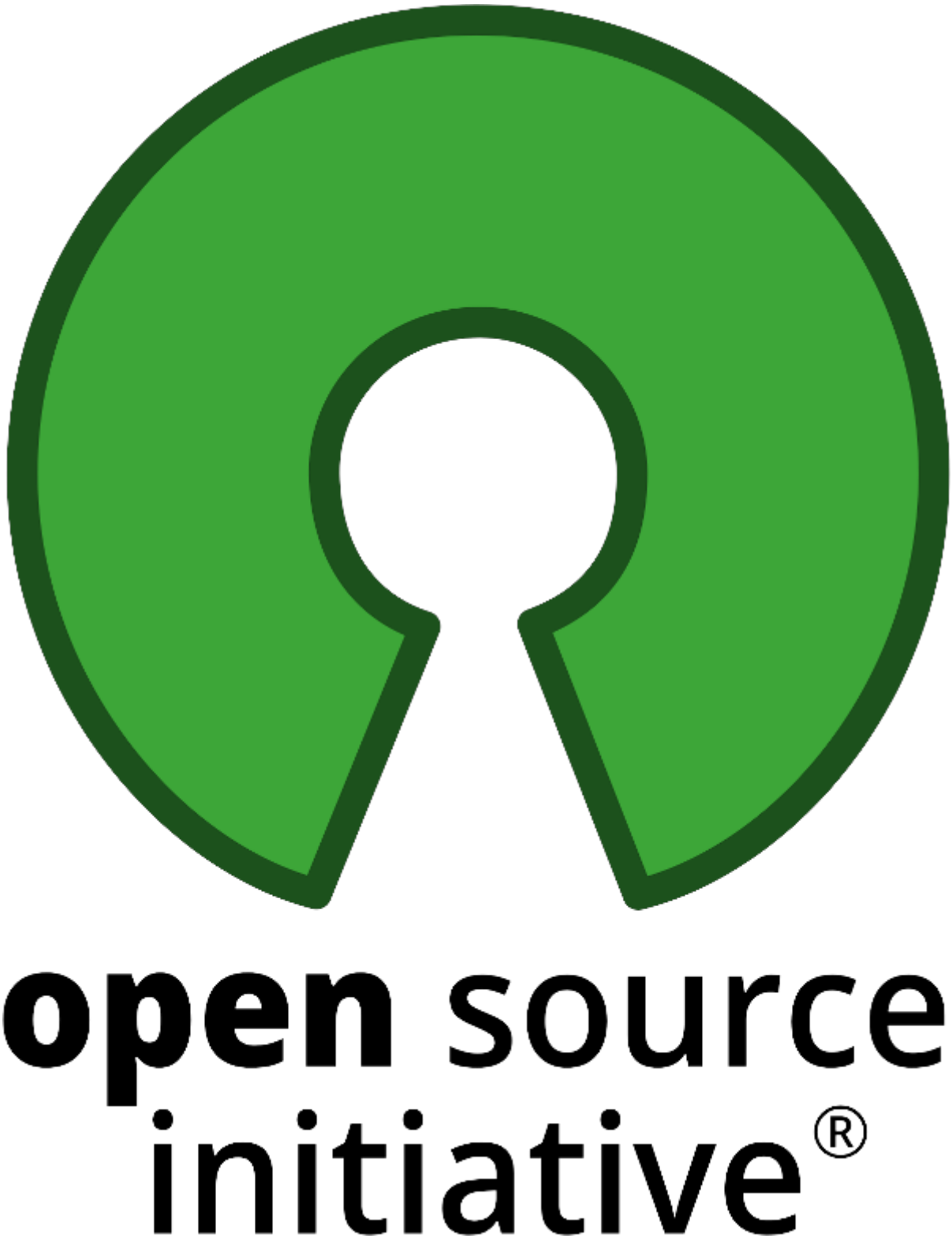
This is how we evaluate software.

How to identify safe open source applications

Open source vs freeware

We have tested the software described here.

https://github.com/ossf/wg-best-practices-os-developers/blob/main/docs/Concise-Guide-for-Evaluating-Open-Source-Software.md
^ helpful



Assessment

Verify authenticity

Consider necessity. every new service increases the attack surface

Open source license type

Does the software require an account, especially one that requires you to provide information like your name or email? Many oss rely on email to build a community by few reputable projects require them.

Typosqiatting obs

Privacy statement

Maintenance & Sustainability

Is there a docker image?

Is it developer created community created or user created?

Activity level

Active community

Open to feedback

Regular updates

Multiple developers

Alpha , beta, stable,

How old is the project

Do they have a testing channel or just main

Is the software a proof of concept or a refined software model?

Maintainers and developers are after unpaid. They are passion projects. While some open source software is funded by foundations, many are small community projects that are self funded by donations.

Code quality reports, code maintenance

Is it maintained

GitHub badges. Is it compiling? Etc

Do they offer a way to deploy using docker?

Usability & Security

Assessment framework

Security vs convenience

Ux/ui

Trusted repository such as GitHub or gitlab

Security audits

Security Through Transparency

It’s How You Implement Software That Matters

Certifications

Secure defaults

Security is not necessarily incorporated into the design and development of OSS.

Many large organizations support OSS projects. However, these projects may rely on work conducted by smaller, volunteer-run OSS projects. For smaller OSS projects, volunteers may have less time to fix problems or conduct security testing. Also, these projects may not receive the funding needed to hire expert security auditors.

The blueprints (source code) reveal the layout, but they don’t tell you where the alarm system is located or the combination to the safe.

Can you report vulnerabilities?

Community

DOCUMENTATION: open or private editor docs? Code markup generator

Stability; number of open issue reports and or very active forums

What about the forums? Are they publicly accessible

How much do they ask for support and in what ways? Are they building community or exploiting it?

What is their community like? Where is it located? Reddit vs forum

Do they meet in person

History of development team

Company or community group

Business or consumer focused

Mission, vision, statement

What is the diversity of the developers

Are they open to outside contribution?

Revision #13
Created 6 May 2025 06:23:53 by metaphorraccoon
Updated 8 June 2025 00:54:29 by metaphorraccoon