Ruby - Feature #19066

Enable Scorecard Github Action

10/17/2022 07:13 PM - joycebrum (Joyce Brum)

Status:	Closed	
Priority:	Normal	
Assignee:	hsbt (Hiroshi SHIBATA)	
Target version:		

Description

Hi, I am Joyce and I'm working on behalf of Google and the Open Source Security Foundation to help essential open-source projects improve their supply-chain security.

Would you consider adopting an OpenSSF tool called Scorecards? Scorecards runs dozens of automated security checks to help maintainers better understand their project's supply-chain security posture. It is developed by the OpenSSF, in partnership with GitHub.

Considering how Ruby project is largely used, it is important to guarantee a good security posture for the project. The scorecard tool can help you on identifying what are the security practices that would improve the project's supply-chain security and what you have to do to accomplish them.

To simplify maintainers' lives, the OpenSSF has also developed the Scorecard GitHub Action. It is very lightweight and runs on every change to the repository's main branch. The results of its checks are available on the project's security dashboard, and include suggestions on how to solve any issues (some examples are attached). The Action does not run or interact with any workflows, but merely parses them to identify possible vulnerabilities. This Action has been adopted by 1800+ projects already, having some prominent users like Tensorflow, Angular, Flutter, sos.dev and deps.dev.

Would you be interested in a PR which adds this Action? Optionally, it can also publish your results to the OpenSSF REST API, which allows a badge with the project's score to be added to its README.

In case of doubts or concerns you can try to check Scorecards FAQ or just reach out to me.

History

#1 - 10/20/2022 08:42 AM - hsbt (Hiroshi SHIBATA)

- *Status changed from Open to Assigned*
- *Assignee set to hsbt (Hiroshi SHIBATA)*

Hi, @joycebrum, Thanks to introduce Scorecards.

I try to setup scorecards action on ruby/ruby repository at first.

#2 - 10/20/2022 01:10 PM - joycebrum (Joyce Brum)

Sure, feel free to explore it. It is very simple to enable, to be honest. If you need some help, feel free to reach out to me.

#3 - 11/11/2022 09:51 PM - hsbt (Hiroshi SHIBATA)

- *Status changed from Assigned to Closed*

I added ossf/scorecards at https://github.com/ruby/ruby/pull/6716.

Thanks for introducing that. We will triage these alerts.

#4 - 11/12/2022 10:28 PM - retro (Josef Šimánek)

Btw. it was recently added to rubygems and rubygems.org as well.

https://github.com/rubygems/rubygems/pull/6055
https://github.com/rubygems/rubygems.org/pull/3258

Files

token-permission.png	571 KB	10/17/2022	joycebrum (Joyce Brum)
security-dashboard.png	620 KB	10/17/2022	joycebrum (Joyce Brum)