

Why you shouldn't use Sails.js

This article was originally published at

<https://gist.github.com/joepie91/cc8b0c9723cc2164660e>.

This article was published in 2015. Since then, the situation may have changed, and this article is kept for posterity. You should verify whether the issues still apply when making a decision

A large list of reasons why to avoid Sails.js and Waterline: <https://kev.inburke.com/kevin/dont-use-sails-or-waterline/>

Furthermore, the CEO of Balderdash, the company behind Sails.js, stated the following:

“

“we promise to push a fix within 60 days”,

@kevinburkeshyp This would amount to a Service Level Agreement with the entire world; this is generally not possible, and does not exist in any software project that I know of.

Upon notifying him in the thread that I actually offer [exactly that guarantee](#), and that his statement was thus incorrect, he accused me of "starting a flamewar", and proceeded to [delete my posts](#).

UPDATE: The issue has been [reopened](#) by the founder of Balderdash. Mind that this article was written back when this was not the case yet, and judge appropriately.

He is apparently also unaware that Google Project Zero expects the exact same - a hard deadline of 90 days, after which an issue is publicly disclosed.

Now, just locking the thread would have been at least somewhat justifiable - he might have legitimately misconstrued my statement as inciting a flamewar.

What is **not** excusable, however, is removing my posts that show his (negligent) statement is wrong. This raises serious questions about what the Sails maintainers consider more important:

their reputation, or the actual security of their users.

It would have been perfectly possible to just leave the posts intact - the thread would be locked, so a flamewar would not have been a possibility, and each reader could make up their own mind about the state of things.

In short: **Avoid Sails.js. They do not have your best interests at heart, and this could result in serious security issues for your project.**

For reference, the full thread is below, pre-deletion.

Write and publish responsible disclosure policy #2830

Closed kevinburkeshyp opened this issue on Apr 10 · 8 comments

kevinburkeshyp commented on Apr 10

- If I find a critical vulnerability in Sails how should I communicate it to the core team?
- What guarantees are given about time to a patch?
- Will reporters be credited for their work in finding a vulnerability?
- How are critical security vulnerabilities disclosed to the community?
- Are vulnerabilities given a CVE number?
- Once you write a page like this, [how can I be expected to find it?](#)

Here is an example of what a page like this should look like: <http://docs.python-requests.org/en/latest/community/vulnerabilities/>

Labels

- needs documentat...
- needs review

Milestone

No milestone

Assignee

irinathan

Notifications

Unsubscribe

You're receiving notifications because you were mentioned.

5 participants

particlebanana commented on Apr 10 Owner

As mentioned in the Waterline issue this would be great.

irinathan was assigned by **particlebanana** on Apr 10

tjwebb added **needs documentation** **needs review** labels on Apr 11

tjwebb commented on Apr 11 Collaborator

@**kevinburkeshyp** excellent suggestion, thanks.

What guarantees are given about time to a patch?

We try in earnest to resolve critical issues as soon as possible. Like any project -- open-source or proprietary -- we operate with finite resources. If your business would like an SLA, that can be set up through <http://balderdash.co>.

This was referenced on Apr 11

Write and publish responsible disclosure policy balderdashy/sails-postgres#149 **Closed**

Write and publish responsible disclosure policy balderdashy/waterline#945 **Closed**

kevinburkeshyp commented on Apr 13

Understood, and it's fine if the policy is so long in the future as "we promise to push a fix within 60 days", just communicating expectations is a good thing for people reporting issues.

tjwebb commented on Apr 14 Collaborator

"we promise to push a fix within 60 days".

@**kevinburkeshyp** This would amount to a Service Level Agreement with the entire world; this is generally not possible, and does not exist in any software project that I know of. Again, if you need an SLA on turnaround for specific issues, contact me separately.

Aside from that, it's a good idea to be clearer in the documentation about how to report security issues, and how we will handle them.

kevinburkeshyp commented on Apr 14

Not necessarily asking you to guarantee some kind of SLA.

I'm just asking for, like, if someone comes to you with "there is a query string that will crash the Node process for every sails user" or "I found a SQL injection attack that allows a full database dump for anyone that's using waterline", if that person doesn't hear back from you, they are going to get antsy, worry that someone else will find it/exploit it, possibly decide to go public before a patch has been prepared, etc.

I know open source is a volunteer thing, but, I don't think "we will respond to your security disclosure within 14[30]60 days" is an unreasonable burden.

CWyrzten commented on Aug 5 Collaborator

Did the comments and PR cover the issue? Can we close this up? It will always be searchable and can be reopened for discussion at any time, of course?

joepie91 commented 10 hours ago

@**tjwebb**: This would amount to a Service Level Agreement with the entire world; this is generally not possible, and does not exist in any software project that I know of.

I provide such a guarantee for all of my projects, actually:

Found a security vulnerability in any of my code? E-mail me at security@crypto.net. A 48 hour response time is guaranteed. A 48 hour patch timeframe is guaranteed where physically possible for me to do so (nearly all cases). I take security seriously.

It's just a matter of keeping up the quality of your codebase, so that any issues can be fixed quickly. Well-modularized code should not take a lot of time to fix, even if sizeable, and security / data loss issues should be right at the very top of your priority list.

tjwebb commented 2 hours ago Collaborator

I provide such a guarantee for all of my projects, actually

Well-modularized code should not take a lot of time to fix, even if sizeable, and security / data loss issues should be right at the very top of your priority list.

Your advice is both obvious and irrelevant. We field hundreds of issues, questions, concerns, bugs, and feature requests every day on Github, Google Groups, Gitter, StackOverflow, etc. We have tens -- if not hundreds -- of thousands of users. Doing Smart Things does not in itself make managing a project used by startups, hackathons, and fortune 500 companies all over the world quite as magically simplistic as you make it out to be.

Let's stay on topic. @**kevinburkeshyp** has a valid question and makes a good point. I'm open to suggestions on how best to manage the disclosure process. Claiming that we'll fix every security issue immediately is not realistic, and I'm not going to commit to something that I can't deliver on.

joepie91 commented 20 minutes ago

Your advice is both obvious and irrelevant.

My remark is very relevant. You claim that such a guarantee is not possible; that is wrong.

Revision #1

Created 2024-12-11 14:51:20 UTC by joepie91

Updated 2024-12-11 18:44:19 UTC by joepie91