schema-inspector / **schema-inspector** Public

Code | Issues 5 | Pull requests 5 | Discussions | Actions | Projects | ...

ReDoS in Schema-Inspector (email validation)

Moderate **mattwelke** published **GHSA-f38p-c2gq-4pmr** on Mar 13, 2021

Package

schema-inspector (npm)

Affected versions	Patched versions
All version below 2.0.0	2.0.0

Description

Impact

What kind of vulnerability is it? Who is impacted?
Email address validation is vulnerable to a denial-of-service attack where some input (for example `a@0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.`) will freeze the program or web browser page executing the code. This affects any current schema-inspector users using any version to validate email addresses. Users who do not do email validation, and instead do other types of validation (like string min or max length, etc), are not affected.

Patches

Has the problem been patched? What versions should users upgrade to?
Users should upgrade to version 2.0.0, which uses a regex expression that isn't vulnerable to ReDoS. The new regex expression is more limited in what it can check, so it is more flexible than the one used before. Therefore, this was a new major version instead of a new patch version to warn people upgrading that they should make sure the email validation still works for their use case.

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?
If a user chooses to not upgrade, the only known workaround would be to stop using the email validation feature in the library. The user could, for example, accept the email address into their system but save it in a "not yet validated" state in their system until a verification email is sent to it (to determine whether the email is valid and belongs to the form submitter). Note that this is the preferred way of validating email addresses anyways.

References

Are there any links users can visit to find out more?
https://gist.github.com/mattwelke/b7f42424680a57b8161794ad1737cd8f

For more information

If you have any questions or comments about this advisory, you can create an issue in this repository.

Severity

Moderate

CVE ID

CVE-2021-21267

Weaknesses

No CWEs

Credits

erik-krogh