New issue

Jump to bottom

Add advisory for bindata #476

Closed **kuahyeow** opened this issue on Jun 1, 2021 · 7 comments

Labels need clarification

kuahyeow commented on Jun 1, 2021 • edited

Potential DoS (combined with `constantized` - see https://blog.presidentbeef.com/blog/2020/09/14/another-reason-to-avoid-constantize-in-rails/ for background) which was fixed in dmendel/bindata@ `d99f050` as part of bindata 2.4.10

No CVE yet

reedloden commented on Jun 1, 2021 Member

@kuahyeow are you associated with the `bindata` project? If so, you can request a CVE via the GitHub Security Advisory process. Otherwise, I can ask GitHub to assign a CVE.

kuahyeow commented on Jun 1, 2021 Author

@reedloden No, I am not associated with the `bindata` project. (For transparency, I am part of the GitLab team that found and reported this issue to the `bindata` mantainer - see also https://about.gitlab.com/releases/2021/06/01/security-release-gitlab-13-12-2-released/#update-bindata-dependency)

> Otherwise, I can ask GitHub to assign a CVE.

Yes, that will be good, thanks!

rschultheis commented on Jun 16, 2021 • edited Contributor

Hello, I am with the GitHub Security Lab team. We are evaluating this to see if assigning a CVE makes sense CC **@reedloden** . Can someone articulate the security impact more clearly? The linked blog article discusses the use of `constantize` creates a memory leak, but in the linked commit there is not any code change involving `constantize` .

Is the "Potential DoS" simply due to the previous implementation being inneficient?

CC **@kuahyeow** could we get just a bit more details?

postmodern added the need clarification label on Jun 16, 2021

kuahyeow commented on Jun 21, 2021 Author

Hello **@rschultheis**, thanks for reaching out.

I think since this is public information, I can expand on the details. The issue is that it was extremely slow for certain classes in BinData to be created. For example `BinData::Bit100000` , `BinData::Bit100001` , `BinData::Bit100002` , `BinData::Bit<N>`

So this, in combination with `<user_input>.constantize` means we have a (slow) CPU-based DoS. Note this is not an issue with BinData gem by itself - attacker needs to find a place where user input is used with `constantize` in the application.

Does this make sense ?

rschultheis commented on Jun 23, 2021 Contributor

@kuahyeow yes that makes sense thanks. I've gone ahead and submited `CVE-2021-32823` for this advisory with a CVSS of `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L` / low.

We have also published GHSA-hj56-84jw-67h6 for this.

rschultheis mentioned this issue on Jun 23, 2021

add CVE-2021-32823 for bindata #483

Merged

rschultheis commented on Jun 23, 2021 Contributor

Also I made this PR to add this advisory to this repo: #483

1

reedloden commented on Jun 23, 2021 Member

This has been added. Thanks, all!

reedloden closed this as completed on Jun 23, 2021

 **Gerst20051** mentioned this issue on Jun 24, 2021

Update Bindata Dependency Due To Security Issue nov/json-jwt#94

Closed

Assignees

No one assigned

Labels

need clarification

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants