

[New issue](#)[Jump to bottom](#)

GitLab webhook event validator vulnerable to timing attacks

#2391

✓ Closedcedws opened this issue on Jul 14 · 1 comment · Fixed by [#2392](#)

Labels

security

cedws commented on Jul 14

Contributor

Community Note

- Please vote on this issue by adding a 👍 [reaction](#) to the original issue to help the community and maintainers prioritize this request. Searching for pre-existing feature requests helps us consolidate datapoints for identical requirements into a single place, thank you!
- Please do not leave "+1" or other comments that do not add relevant new information or questions, they generate extra noise for issue followers and do not help prioritize the request.
- If you are interested in working on this issue or have submitted a pull request, please leave a comment.

Overview of the Issue

I was just passing through the code and noticed that the GitLab webhook event validator code does not use a constant time comparison function to validate the webhook secret. In theory it would be possible to use a timing attack to recover this secret as an attacker and then forge webhook events. GitHub and Bitbucket event validator code is not vulnerable because they make use of HMACs as far as I can see.

The risk of this being exploited is probably fairly low so I think it's safe to report publicly like this.

[atlantis/server/controllers/events/gitlab_request_parser_validator.go](#)

Lines 62 to 67 in e153cea

```
62 // Validate secret if specified.
63 headerSecret := r.Header.Get(secretHeader)
64 secretStr := string(secret)
65 if len(secret) != 0 && headerSecret != secretStr {
66     return nil, fmt.Errorf("header %s=%s did not match expected secret", secretHeader, h
67 }
```

I will follow up with a PR to fix this shortly.

  **cedws** added the `bug` label on Jul 14

  **cedws** mentioned this issue on Jul 14

fix: use constant time comparison of webhook secret in gitlab event validator #2392

 Merged

  **chenrui333** added `security` and removed `bug` labels on Jul 15

 **lilincmu** closed this as completed in [#2392](#) on Jul 15

lkysow commented on Jul 15

Member

Thanks @cedws! In the future just a heads up that we have a different process for security issues:
<https://github.com/runatlantis/atlantis/blob/master/CONTRIBUTING.md#reporting-security-issues>

  **GoVulnBot** mentioned this issue on Jul 29

**x/vulndb: potential Go vuln in github.com/runatlantis/atlantis/server/controllers/events:
CVE-2022-24912 golang/vulndb#534**

 Closed

  **jba** mentioned this issue on Jul 29

x/vulndb: potential Go vuln in Path is unknown: CVE-2022-24912 [jba/nested-modules#383](#)

 Open

Assignees

No one assigned

Labels

`security`

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 **fix: use constant time comparison of webhook secret in gitlab event validator**
cedws/atantis

3 participants

