

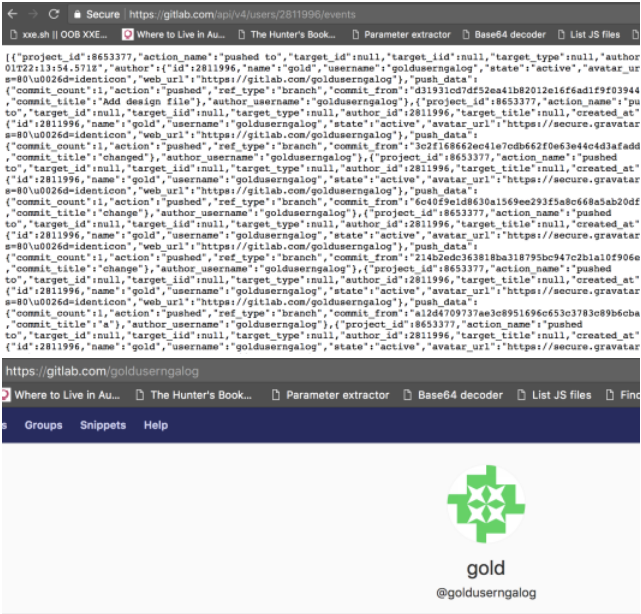
User's activity-related personal information are exposed in API event response even enabled private profile

Link: <https://hackerone.com/reports/417725>
By: @ngalog

Details: Docs link: <https://gitlab.com/help/user/profile/index.md#private-profile>

PoC:

- <https://gitlab.com/golduserngalog> has no user activities shown in response
- But <https://gitlab.com/api/v4/users/2811996/events> show my personal activity anyway



This user has a private profile

Impact

User's activity-related personal information are exposed in API event response even enabled private profile

📎 Drag your designs here or [click to upload](#)

Tasks @0


No tasks are currently assigned. Use tasks to break down this issue into smaller parts.


Linked items 2


Relates to


- [Contributed projects info is still visible even user enable private profile](#)
gitlab-foos#52677 11.7 Jan 14, 2019
- [KR: Close 15 Security issues across quarter \(ManageAccess\) => 100%](#)
gitlab-com/www-gitlab-com#7714 Jul 31, 2020


Activity


 James Ritchey added priority 3 severity 3 scoped labels 4 years ago


 James Ritchey @Ritchey 4 years ago
/cc @gl-security @stanhu @DouweM @smcniel
Edited by James Ritchey 4 years ago


 James Ritchey added Create (DEPRECATED) label 4 years ago


 Douwe Maan @DouweM 4 years ago
/cc @lmcandrew @jeremy


 Douwe Maan added Manage (DEPRECATED) label and removed Create (DEPRECATED) label 4 years ago


 Liam McAndrew added bug scoped label 4 years ago


 Jeremy Watson (ex-GitLab) mentioned in issue gitlab-ce#52677 4 years ago

 James Ritchey marked this issue as related to gitlab-ce#52677 4 years ago

 GitLab SecurityBot changed due date to January 4, 2019 4 years ago

 Jeremy Watson (ex-GitLab) changed milestone to 11.8 4 years ago

 Jeremy Watson (ex-GitLab) changed milestone to 11.7 4 years ago

 GitLab Bot added Accepting merge requests label 4 years ago

Please [register](#) or [sign in](#) to reply