Closed Opened 9 months ago by **David Smith** 🌴

Incident Review for gitlab-org/gitlab project 404 / accidental delete

Incident: production#1183 (closed)

Summary

- Service(s) affected : gitlab-org/gitlab
- Team attribution :
- Minutes downtime or degradation : 1h50m

For calculating duration of event, use the Platform Metrics Dashboard to look at appdex and SLO violations.

Impact & Metrics

- What was the impact of the incident? (i.e. service outage, sub-service brown-out, exposure of sensitive data, ...)
  - gitlab-org/gitlab was inaccessible
- Who was impacted by this incident? (i.e. external customers, internal customers, specific teams, ...)
  - Internal customers, external contributors
- How did the incident impact customers? (i.e. preventing them from doing X, incorrect display of Y, ...)
  - Internal customers and external contributors were unable to access the project, submit MR's, or perform any action against it.
- How many attempts were made to access the impacted service/feature?
  - N/A
- How many customers were affected?
  - N/A
- How many customers tried to access the impacted service/feature?
  - N/A

Detection & Response

- How was the incident detected?
  - Human/manual detection
- Did alarming work as expected?
  - No, there may not be any alarming for this type of incident
- How long did it take from the start of the incident to its detection?
  - Immediately detected
- How long did it take from detection to remediation?
  - Approx 1h50m
- Were there any issues with the response to the incident? (i.e. bastion host used to access the service was not available, relevant team memeber wasn't page-able, ...)
  - No issues. On-call was already engaged due to a different incident and was immediately available.

Root Cause Analysis

5 Why's - Merge Request Management

1. gitlab-org/gitlab project was deleted from gitlab.com
2. A copy/paste error led to the API call to delete the project.
3. The API delete merge request was attempted via the API
4. It was believed that merge requests could not be deleted through the GitLab UI

5 Why's - Confidential Commits/MR's

1. gitlab-org/gitlab project was deleted from gitlab.com
2. The API delete function was manually executed using a global administrator token while attempting to delete a merge request on the GitLab project
3. Confidential data (security vulnerability fix) was pushed to the public repo on GitLab.com
4. Automated measures to prevent security vulnerability fixes from being pushed (publicly) to GitLab.com not in place, dependent on manual steps (security harness) by the individual Dev's.

5 Why's - Erroneous API Command

1. gitlab-org/gitlab project was deleted from gitlab.com
2. The API delete function was manually executed using a global administrator token while attempting to delete a merge request on the GitLab project
3. The copy/paste of said curl command had an accidental line break
4. There was seemingly no way to delete an MR via the interface so a curl command was crafted

What went well

- Oncall was already around and response was immediate.
- A lot of people jumped in to help

What can be improved

1. We didn't clearly follow the escalation process for getting oncall engineering staff on the zoom - not infra, but how we engage engineering help after incident start. We had many engineers join (and thank you for that), but we could have been more crisp in going through the escalation process. Contributing factors - this was off primary hours for the US people who were pulled into the call. Re-reviewing with incident/infra managers to see what we can do to keep engineering oncall easy to access.
2. 1h50m is a long time to correct. Watching from the zoom, it became clear after we restarted sidekiq and the project again began to 404 that we did not fully understand what happens when a project is marked for deletion.
3. We got lucky - the delete job ultimately threw an exception and could not successfully delete the project in 1 transaction. This left us a state that was much easier to recover from. We should not count on this luck in the future.
4. Other than the secrecy of admin/owner API tokens there's no intentional measures in place to prevent the deletion of a project by an admin or owner.
5. The documentation for security fixes being on dev and about the "security harness" should be improved.

Corrective actions

- Until process improvements for confident MR's on GitLab.com are in place, @pharrison is creating a script to simplify MR deletions to prevent this specific scenario from recurring. https://gitlab.com/gitlab-com/gl-security/secops/operations/issues/420
- Implement option to prevent deletion of project: gitlab-org/gitlab#32647
- Audit admin tokens and their expiration: https://gitlab.com/gitlab-com/gl-infra/infrastructure/issues/8023
- Improve runbooks on accidental project deletion to include information about sidekiq and what to do to try to cancel an in-flight request: #8025
- ~~Create backup before deletion: gitlab-org/gitlab#33085 (closed)~~
- ~~Configurable instance-wide deletion delay: gitlab-org/gitlab#33095 (closed)~~
- Take backup before deletion and deletion delay: gitlab-org/gitlab#27301 (closed)

Guidelines

- Blameless RCA Guideline
- 5 whys

Edited 9 months ago by Alex Hanselka

Linked issues ❓ 5

Relates to

⊖ gitlab-org/gitlab project returning 404
production#1183

○ Prevent accidental disclosure of security changes by disallowing pushes to non-topic branches
delivery#350

⊖ Automatically backup project before deletion
gitlab-org/gitlab#33085

○ Update Runbooks to be more useful during an accidental project deletion.
#8025

○ Implement checkbox (or other) to make deletion of a project opt-in
gitlab-org/gitlab#32647

David Smith 🌴 @dawsmith marked this issue as related to production#1183 (closed)
9 months ago

Chris Hill @chill104 · 9 months ago

Sorry this happened - I believe the lag time between when a project or group is marked for delete and when it's actually deleted needs to be much longer (i.e. 24 hours) or the recovery from a deleted project needs to be much shorter.

Collapse replies

John Jarvis @jarv · 9 months ago Owner

> I believe the lag time between when a project or group is marked for delete and when it's actually deleted needs to be much longer

🤔 For delaying deletions I can see how this may cause some pain, even if it was configurable I don't know if we would want to set it for all projects on gitlab.com.

I really like @T4cC0re suggestion of something like "termination protection" for important projects gitlab-org/gitlab#32647

For recovery I think having a backup prior to deletion would be a really nice feature.

Chris Hill @chill104 · 9 months ago

> For recovery I think having a backup prior to deletion would be a really nice feature.

Agreed, but the backup would have to include "everything" embedded within a project - registry, npm registries, wikis, etc. It's my understanding this is what's holding us back from a speedy recover of projects.

I'm all for everything you're suggesting here.. and I think it warrants significant investment on accidental protection.

Hendrik Meyer @T4cC0re · 9 months ago Maintainer

> For recovery I think having a backup prior to deletion would be a really nice feature.

💯 👍
But I also think a 'mark before delete' is a good idea, too. If that happens to be lets say 72h (because of weekends), we would also have enough time to grab a backup and archive it somewhere. In that case we can at least restore everything, even if not speedy.

We would of course have to tell that to the customer, and maybe even give them an option to opt-out from that safety backup.

Please register or sign in to reply

Alex Hanselka @ahanselka mentioned in issue gitlab-org/gitlab#32623 9 months ago

John Woods 💬 @jwoods06 mentioned in issue gitlab-org/gitlab#27301 (closed) 9 months ago

Paul Harrison @pharrison changed the description 9 months ago

John Jarvis @jarv · 9 months ago Owner

@dawsmith who do you think will be the DRI for this RCA? I think a few things we should consider are:

- Auditing admin keys on a regular basis, can we ensure that all personal access tokens belonging to admins have expiration and audit regularly? Maybe the security team would help out with this?
- Maybe take another look at runbooks for what to do when there is an an accidental deletion and in situations like this where we need to kill sidekiq jobs
- I like the deletion protection proposal, perhaps we also should consider taking backups before deletion as the default with an override to disable?

Collapse replies

David Smith 🌴 @dawsmith · 9 months ago Owner

Thanks for the ping @jarv - that was a todo for this week. @ahanselka - do you think you could take this before you are out? I can add some comments today and we should try to get some time with @pharrison who had some things to add too.

Also- those are all good suggestions and we should likely have some more exploring safeguards when security needs to take steps for removing commits for a security incident.

David Smith 🌴 @dawsmith · 9 months ago Owner

Added a few comments in what can be improved.

Paul Harrison @pharrison · 9 months ago Maintainer

@dawsmith Added a few comments last week, will add more shortly.

100% agree on the auditing of admin keys for GL.com. I'll open an infra issue to do a DB dump on admin accounts + active tokens.

Paul Harrison @pharrison · 9 months ago Maintainer

@dawsmith created https://gitlab.com/gitlab-com/gl-infra/infrastructure/issues/8023 to begin the account audit.

Alex Hanselka @ahanselka · 9 months ago Owner

I've labeled https://gitlab.com/gitlab-com/gl-infra/infrastructure/issues/8023 as a corrective action and added it to the list.

Alex Hanselka @ahanselka · 9 months ago Owner

> I like the deletion protection proposal, perhaps we also should consider taking backups before deletion as the default with an override to disable?

What do we think this would look like? I made gitlab-org/gitlab#33085 (closed) about it. I was thinking that it would just use the import/export feature to generate a backup and email the user issuing the delete with the link, just as if the user had clicked the export button. Then, if the backup succeeds it will proceed onward to deletion. If the backup fails, it will abort the delete as well.

Paul Harrison @pharrison · 8 months ago Maintainer

40 active Admin API tokens on GitLab.com as of 20191008. I'll be burning through the list to confirm their necessity: https://docs.google.com/spreadsheets/d/1yczQdSLJq3pik8ctK5VbNgNXizYhHV7L0liRJxodjMs/edit#gid=0

Edited by Paul Harrison 8 months ago

Please register or sign in to reply

David Smith 🌴 @dawsmith changed the description 9 months ago

Paul Harrison @pharrison changed the description 9 months ago

Paul Harrison @pharrison · 9 months ago Maintainer

On "What can be improved" num. 1; engaging on-call. I had already paged on-call to assist with the pipeline deletes (re: https://gitlab.com/gitlab-com/gl-security/secops/operations/issues/414) and was still speaking when the delete occurred, which is why I did not page again.

Edited by Paul Harrison 9 months ago

Collapse replies

David Smith 🌴 @dawsmith · 9 months ago Owner

Makes sense @pharrison - I was more referring to how we pulled in the rest of engineering, not you. The manager on call (Me) should have more specifically followed this page and gone to #dev-esclation. @DylanGriffith did post there, but it probably should have come from the infra on call people. We got by, but I wanted to acknowledge we didn't perfectly follow process

David Smith 🌴 @dawsmith · 9 months ago Owner

I'm thinking more about what we can do to have that front of mind in response.

Please register or sign in to reply

Paul Harrison @pharrison changed the description 9 months ago

Paul Harrison @pharrison changed the description 9 months ago

Paul Harrison @pharrison marked this issue as related to delivery#350 9 months ago

Alex Hanselka @ahanselka mentioned in issue #8025 9 months ago

Alex Hanselka @ahanselka changed the description 9 months ago

Alex Hanselka @ahanselka mentioned in issue gitlab-org/gitlab#33085 (closed) 9 months ago

Alex Hanselka @ahanselka changed the description 9 months ago

David Smith 🌴 @dawsmith added IncidentReview label 9 months ago

David Smith 🌴 @dawsmith added 1 deleted label 9 months ago

David Smith 🌴 @dawsmith assigned to @ahanselka 9 months ago

David Smith 🌴 @dawsmith changed the description 9 months ago

Alex Hanselka @ahanselka marked this issue as related to gitlab-org/gitlab#33085 (closed) 9 months ago

Alex Hanselka @ahanselka marked this issue as related to #8025 9 months ago

Alex Hanselka @ahanselka marked this issue as related to gitlab-org/gitlab#32647 9 months ago

Alex Hanselka @ahanselka changed the description 9 months ago

Alex Hanselka @ahanselka changed the description 9 months ago

Alex Hanselka @ahanselka · 9 months ago Owner

I don't know that we need 5 why's for each of the above. They seem pretty complete as is.

Also, as it turns out, you CAN delete merge requests via the API. I've tested it as an owner of a project and as an admin and it was available for both. I was certain that when I was looking into it the day of the incident that it wasn't an option, but perhaps I just didn't notice? It is also possible the button was missing the day of the incident and was later fixed by an auto-deploy, however this seems less likely.

Alex Hanselka @ahanselka · 9 months ago Owner

I've created gitlab-org/gitlab#33095 (closed) to propose a configurable instance-wide deletion delay. Please feel free to leave comments.

Collapse replies

Jayson Salazar @jdsalaro · 9 months ago Developer

@ahanselka gitlab-org/gitlab#27301 (closed) has existed for a while, IMO that overlaps with your suggestion or will at least include it.

Alex Hanselka @ahanselka · 9 months ago Owner

So firstly, yay thank you for letting me know! Secondly, it is very concerning that this has happened multiple times to both customers AND ourselves and that issue seems to have almost no traction.

Please register or sign in to reply

Alex Hanselka @ahanselka changed the description 9 months ago

Alex Hanselka @ahanselka changed the description 9 months ago

Alex Hanselka @ahanselka · 9 months ago Owner

I closed my two issues I made and just linked to gitlab-org/gitlab#27301 (closed). It contains both my issues, so it seemed useless to have more than just that one.

Alex Hanselka @ahanselka changed the description 9 months ago

Alex Hanselka @ahanselka changed the description 9 months ago

Alex Hanselka @ahanselka · 8 months ago Owner

I think it should be safe to close this now as it seems complete and corrective actions have been created.

Alex Hanselka @ahanselka closed 8 months ago

ops-gitlab-net @ops-gitlab-net mentioned in issue #8253 (closed) 8 months ago

Rachel Nienaber @rnienaber · 8 months ago Developer

Adding wg-isolation because we needed to restart sidekiq to resolve this and in this instance, we were the noisy neighbours.

Rachel Nienaber @rnienaber added wg-isolation label 8 months ago

Anthony Sandoval @AnthonySandoval added team Reliability scoped label 6 months ago

Anthony Sandoval @AnthonySandoval removed 1 deleted label 6 months ago

Please register or sign in to reply