Starred by 2 users

Owner: ----

CC: llvm-security@googlegroups.com

Status: Done *(Closed)*

Components: ----

Modified: 4 hours ago

Security
Restrict-View-SecurityTeam

Your Hotlists: Update your hotlists

Issue 39: Github PAT of contributor leaked

Reported by sergej.frank89@gmail.com on Sat, Apr 1, 2023, 12:27 PM GMT+1

Code

1 of 6
Back to list

Only users with SecurityTeam permission or issue reporter may view.

Description #2 by peter.smith@arm.com (3 days ago)

The GitHub Personal Access Token (PAT) of user `[[redacted]]` has been leaked in a Docker Hub image. This is a serious security concern, as the user has push rights to several repositories, which are listed below:

llvm-project
llvm-lnt
llvm-test-suite
llvm-www
llvm-zorg
circt
torch-mlir
vscode-mlir

llvm.jpg Delete
143 KB View Download

Comment 1 by oliver@apple.com on Sun, Apr 2, 2023, 12:10 AM GMT+1 Project Member

In theory posting the GAT to a gist would be sufficient for GitHub to revoke it

Comment 2 by oliver@apple.com on Sun, Apr 2, 2023, 1:08 AM GMT+1 Project Member

Is there anyone from llvm.org who has access to security reports? (raising the question of why the security component is separated from the main llvm.org bug tracker infrastructure :-/)

Comment 3 by sergej.frank89@gmail.com on Sun, Apr 2, 2023, 3:08 PM GMT+1

Yeah, I thought about it too. But its a bit too risky for me to post the PAT :)
Not sure if github is fast enough and no other scraper would get it before them.

Comment 4 by kristof.beyls@arm.com on Mon, Apr 3, 2023, 9:21 AM GMT+1 Project Member

I've let the admins of the LLVM github area know about this report.
I wonder if you could share some more evidence that the access token did get leaked?

Comment 5 by sergej.frank89@gmail.com on Mon, Apr 3, 2023, 10:55 AM GMT+1

it was included in a Docker image that the user published on Dockerhub. If you now look at the individual instructions of the layer, you can extract it there. I can't currently think of a way to share more information with you without making the token itself visible to you. the attached screenshot shows the user's authorisation to repos within the llvm org.

Comment 6 by dimitry@andric.com on Mon, Apr 3, 2023, 11:07 AM GMT+1 Project Member

Btw, last time I looked there were almost 2900 people in the GitHub llvm organization (see https://github.com/orgs/llvm/people), so are we going to be able to check each and every one of those people's access permissions? Not all of those will have permission to push to llvm-project itself, but still, there are so many committers that it is almost certain that *some* of their accounts, passwords and/or access tokens are compromised.

I.e. what is our policy in general for this?

Comment 7 by kristof.beyls@arm.com on Mon, Apr 3, 2023, 4:17 PM GMT+1 Project Member

The admins of the LLVM github organization have confirmed that commit access for this user has been removed.
I am reaching out to the user to explain what happened and to give them an opportunity to get their commit access back after taking appropriate steps.

@Dimitry: I think the discussion about changing policy around this can be held in public, e.g. on LLVM Discourse. My understanding of the most likely way forward is for the LLVM project to move code review to GitHub Pull Requests, which then enables workflows where far fewer people have commit/push/merge rights.

Comment 8 by paul.robinson@sony.com on Mon, Apr 3, 2023, 4:24 PM GMT+1 Project Member

I agree with Kristof that the policy discussion can take place on Discourse.
I have opinions but they are better suited for that policy discussion than here.

Comment 9 by sergej.frank89@gmail.com on Mon, Apr 3, 2023, 4:48 PM GMT+1

do you have a contact to this person? i just saw that the token has access to various amd repos.
do you need any more information from me?

Comment 10 by sergej.frank89@gmail.com on Mon, Apr 3, 2023, 4:53 PM GMT+1

However, I can confirm that the token no longer has push rights to the LLVM repos.

Comment 11 by mattdr@google.com on Mon, Apr 3, 2023, 6:02 PM GMT+1 Project Member

I think it would be reasonable to email `security@github.com` and have them revoke the PAT.

As comment #1 points out, this would happen if you pushed it to a public repo; doing it by email seems slightly nicer.

Comment 12 by kristof.beyls@arm.com on Fri, Apr 21, 2023, 7:44 AM GMT+1 Project Member

I've just heard confirmation from the owner of the leaked token that the token should be unusable.

Comment 13 by kristof.beyls@arm.com on Wed, May 17, 2023, 10:35 AM GMT+1 Project Member

Status: Done (was: New)
Labels: -Restrict-View-SecurityTeam

Comment 14 by peter.smith@arm.com on Thu, Jan 18, 2024, 5:23 PM GMT (3 days ago) Project Member

Description was changed.

Comment 15 by peter.smith@arm.com on Mon, Jan 22, 2024, 9:45 AM GMT (4 hours ago) Project Member

Labels: Restrict-View-SecurityTeam

Adding back Restrict-View-SecurityTeam in preparation for transparency report. A new ticket will be created with a PDF copy of this issue (with the new description) which can be mentioned in the transparency report.

Add a comment and make changes

Please keep discussions respectful and constructive. See our code of conduct.

Add a comment

Add attachments Drop files here to add them (Max: 10.0 MB per comment)

Summary: Github PAT of contributor leaked
Status: Done = The requested non-coding task was completed
Owner:
CC: llvm-security@googlegroups.com
Components:
BlockedOn:
Blocking:
Labels: Security, Restrict-View-SecurityTeam

Save changes Discard Send email