CocoaPods trunk is moving to be read-only. Read more on the blog (https://blog.cocoapods.org/CocoaPods-Specs-Repo/), there are 2 months to go.

CocoaPods Trunk: 3 Remote Code Execution found, 2023



Orta Therox (https://twitter.com/orta)

28 October 2023

Follow @orta

Over the last month, security researchers at evasec.io (https://evasec.io) have been reached out to us about three separate vulnerabilities in CocoaPods Trunk (the server which handles updates to Pods). We've been working with evasec to patch these issues as they come up. Looking at all three combined, I felt we needed to reset all user sessions again, which is why I'm writing on the blog post instead of working on Puzzmo (https://www.theverge.com/23929222/puzzmo-newspaper-games-crossword-zach-gage) which just shipped this week.

There are three key issues reported against Trunk, which were promptly fixed:

- 1. It was still possible to use the 'claim your pod' (https://blog.cocoapods.org/Claim-Your-Pods/) process to take over a Pod when someone had removed all prior maintainers from it
- 2. The email which is sent out to verify your email address can be tricked to change to link to a third party
- 3. The part of trunk which verifies your email address could be used to execute shell commands on the trunk server

Being able to execute arbitrary shell commands on the server gave a possible attacker the ability to read our environment variables, which could be used to write to the CocoaPods/Specs repo and read the trunk database. Being able to trick people into clicking on a link which would take them to a third party site could be used to steal their session keys. I can't guarantee neither of these happened, and I'd rather be on the safe side.

This means you will need to log in again to trunk again to deploy any new Podspecs. If you have automated deployment to CocoaPods working with a stored ENV VAR right now, **this will break**, and you will need to `pod trunk register` again and replace your `COCOAPODS_TRUNK_TOKEN`. We're sorry, I know that sucks, but it also *guarantees* that you are the only person with write access to your pods.

If you are not a pod author, you do not need to do anything.

evasec.io (https://evasec.io) are still in the process of writing up the full technical details of how the exploits worked, so I'll both update this post with links to their write-ups when they are ready, as well as do a new blog post with the details at a higher level to describe how they work to folks who are not intimate with server architectures.

Worst case scenario

Like with the RCE in 2021 (https://blog.cocoapods.org/CocoaPods-Trunk-RCE/) I can't prove these have been actively used. However, just because it hasn't been proved, doesn't mean it hasn't happened. This touches code which has been in trunk since launch, and 9 years is a long time.

The worst case scenario is that an attacker could have used this technique to get access to our trunk database. The trunk database contains the same emails which are public in the git history of the Specs repo. The table of information in the database which should not be seen are session keys. These keys act like unique passwords to accounts, and session keys are used to connect authenticated users to pods. We are wiping all session keys, which ensures no-one other than those with access to their emails can post updates to those pods.

For more information

We want to offer our thanks to evasec.io (https://evasec.io)(EVA) for their thorough reports!

CocoaPods is ran by a set of volunteers in their spare time. If you have any questions or comments about this advisory:

- Open an issue in the trunk repo (https://github.com/CocoaPods/trunk.cocoapods.org)
- Email us at our private security email: info@cocoapods.org (mailto:info@cocoapods.org)

If you're not sure of the email address you used for a pod, use `pod trunk info [pod_name]` to see the connected email accounts.



Follow @orta

(/archived/2022/10-28-CocoaPods-Trunk-RCEs-2023.ma

PREVIOUS POST

CocoaPods Web Hosting now Sponsored by Emerge Tools

By Samuel E. Giddins

(/Web-Hosting-Sponsored-by-Emerge)

NEXT POST

CocoaPods Support & Maintenance Plans

By Orta Therox

(/CocoaPods-Support-Plans)

COCOAPODS IS A PROJECT FROM

Dimitris Koutsogiorgas (https://twitter.com/dnkoutso), Danielle Lancashire (https://dani.builds.terrible.systems/), Eric Amorde (https://github.com/amorde), Igor Makarov (https://github.com/igormaka), Orta Therox (https://orta.io), Paul Beusterien (https://github.com/paulb777), Samuel Giddins (https://segiddins.me), and The CocoaPods Dev Team (https://cocoapods.org/about#team) with contributions from many, many others (https://github.com/CocoaPods/Specs/graphs/contributors).

LOVINGLY SPONSORED BY
Artsy (http://artsy.net), Button (http://www.usebutton.com), Capital One (http://www.capitalone.io), CircleCI (https://circleci.com), Discontinuity (http://discontinuity.eu), Emerge Tools (https://www.emergetools.com), Fingertips (http://www.fngtps.com), Google (https://developers.google.com), Heroku (https://www.heroku.com), jsDelivr (https://www.jsdelivr.com), Realm (https://realm.io), PSPDFKit (https://pspdfkit.com/), RubyMotion (http://www.rubymotion.com), Sauspiel (https://www.sauspiel.de), Slack (https://www.slack.com), SoundCloud (https://www.soundcloud.com), Stripe (https://www.stripe.com), Square (https://www.squareup.com), and Technology Astronauts (http://www.technologyastronauts.ch).