

Mánalogn

Yfirlit yfir árásir á birgðakeðjur





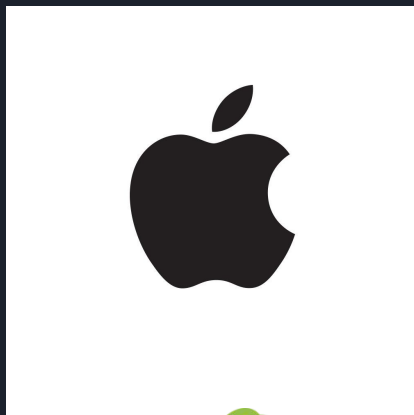
Tímabært Umræðuefni



Microsoft



PayPal



Uber



NETFLIX



Dependency confusion

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack

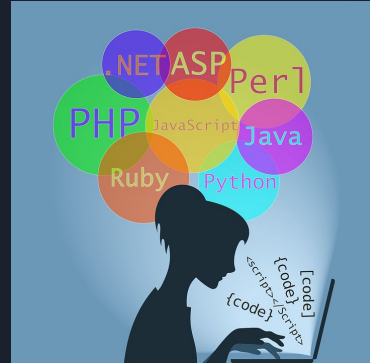
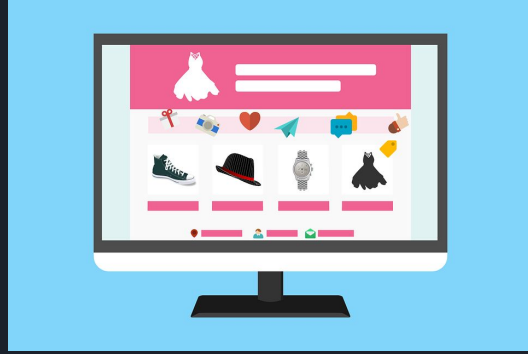


Alex Birsan Feb 9 · 11 min read ★





Dependency Confusion





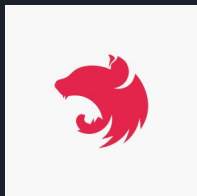
Dependency Confusion



Almenningur



auth-paypal v.9000.0.0



Prívat

auth-paypal v. 2.0.0





Dependency Confusion

```
"dependencies": {  
  "express": "^4.3.0",  
  "dustjs-helpers": "~1.6.3",  
  "continuation-local-storage": "^3.1.0",  
  "pplogger": "^0.2",  
  "auth-paypal": "^2.0.0",  
  "wurfl-paypal": "^1.0.0",  
  "analytics-paypal": "~1.0.0"  
}
```



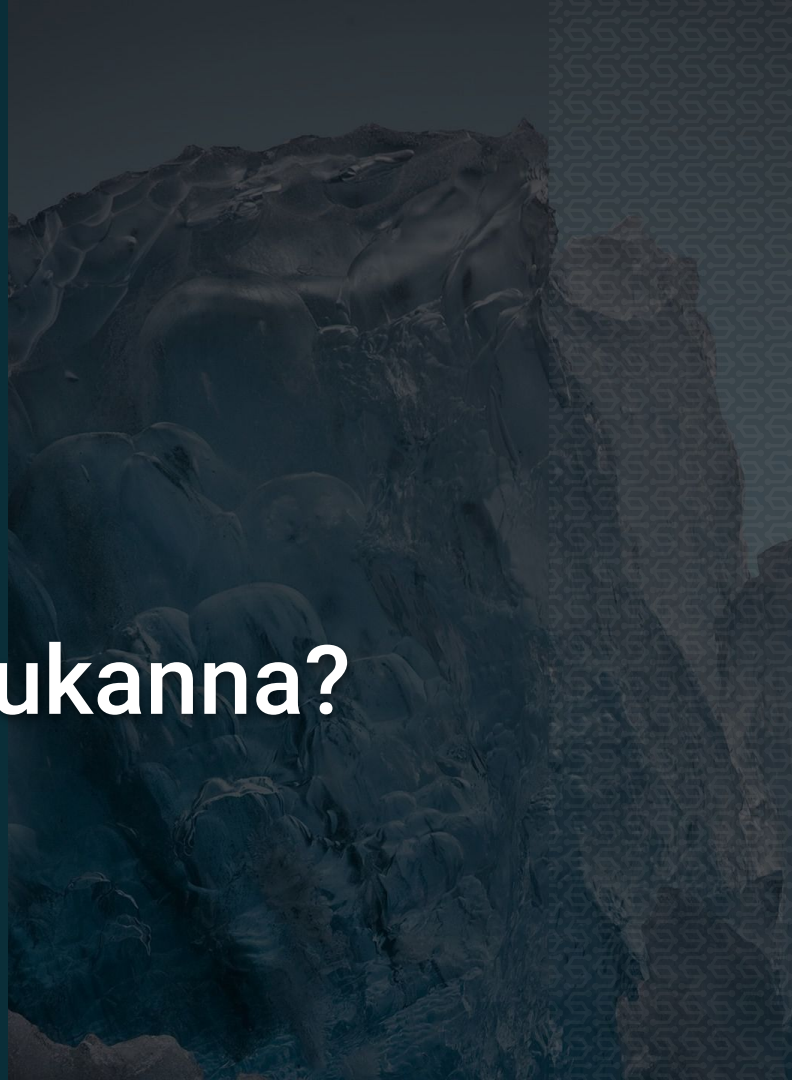
Dependency Confusion

- Pakkastjórar notaðir í árásum





Er þetta að færast í aukanna?






CodeCov 15. apríl

Seinnihluti apríl

The screenshot shows the CodeCov website with a pink and white color scheme. The navigation bar includes links for Product, Solutions, Resources, Pricing, Contact, Login, and a Sign Up button. The main heading is "Bash Uploader Security Update" dated "APRIL 15TH, 2021". A yellow note box contains a warning about a security issue. The "About the Event" section details the incident, the remediation process, and the impact on users.

 Product Solutions Resources Pricing Contact Login [Sign Up](#)

APRIL 15TH, 2021

Bash Uploader Security Update

Note: If you are in the affected user group, at 6 am PT, Thursday, April 15th, we emailed your email address on file from [GitHub](#) / [GitLab](#) / [Bitbucket](#) and added a notification banner in the Codecov application after you log in.

About the Event

Codecov takes the security of its systems and data very seriously and we have implemented numerous safeguards to protect you. On Thursday, April 1, 2021, we learned that someone had gained unauthorized access to our **Bash Uploader** script and modified it without our permission. The actor gained access because of an error in Codecov's Docker image creation process that allowed the actor to extract the credential required to modify our Bash Uploader script.

Immediately upon becoming aware of the issue, Codecov secured and remediated the affected script and began investigating any potential impact on users. A third-party forensic firm has been engaged to assist us in this analysis. We have reported this matter to law enforcement and are fully cooperating with their investigation.

Our investigation has determined that beginning January 31, 2021, there were periodic, unauthorized alterations of our Bash Uploader script by a third party, which enabled them to potentially export information stored in our users' continuous integration (ci) environments. This information was then sent to a third-party server outside of Codecov's infrastructure.

The Bash Uploader is also used in these related uploaders: Codecov-actions uploader for GitHub, the Codecov CircleCI Orb, and the Codecov Bitrise Step (together, the "Bash Uploaders"). Therefore, these related uploaders were also impacted by this event.

The altered version of the Bash Uploader script could potentially affect:

- Any credentials, tokens, or keys that our customers were passing through their CI runner that would be accessible when the Bash Uploader script was executed.
- Any services, datastores, and application code that could be accessed with these credentials, tokens, or keys.
- The git remote information (URL of the origin repository) of repositories using the Bash Uploaders to upload coverage to Codecov in CI.





CocoaPods 20. apríl

Seinnihluti apríl

Hacking 3,000,000 apps at once through CocoaPods

Apr 20, 2021

tl;dr [CocoaPods](#) is a popular package manager used by lots of iOS apps (among other Swift and Objective-C Cocoa applications). I found a remote code execution bug in the central CocoaPods server holding keys for the [Specs repo](#) (<https://trunk.cocoapods.org/>). This bug would have allowed an attacker to poison any package download. [It's fixed now](#).

Introduction

I use the [Signal iOS app](#) to communicate with my friends. I really like Signal, and one of the ways I like to give back to my favorite projects is by trying to find bugs in them.

The first thing that stood out to me when browsing through the [app's source](#) was `Podfile`, which lists Signal's [CocoaPods dependencies](#). I have a long [history with package managers](#), so my first idea was to try and find a bug in the central CocoaPods server. Why hack just Signal if we can find a bug that affects every app using CocoaPods?

The bug

When you upload a package spec to CocoaPods, it tries to make sure you didn't accidentally link to a private repository. It used to do that [like this](#):

```
def validate_git
  # We've had trouble with Heroku's git install, see trunk.cocoapods.org/pull/141
  url = @specification.source[:git]
  return true unless url.include?('github.com') || url.include?('bitbucket.org')


  ref = @specification.source[:tag] ||
    @specification.source[:commit] ||
    @specification.source[:branch] ||
    'HEAD'
  wrap_timeout { system('git', 'ls-remote', @specification.source[:git], ref.to_s) }
end
```





Homebrew 21. apríl


Seinnihluti apríl



Homebrew

Security Incident Disclosure

21 April 2021

 reitermarkus

On 18th April 2021, a security researcher identified a vulnerability in our `review-cask-pr` GitHub Action used on the `homebrew-cask` and all `homebrew-cask-*` taps (non-default repositories) in the Homebrew organization and reported it on our HackerOne.

Whenever an affected cask tap received a pull request to change only the version of a cask, the `review-cask-pr` GitHub Action would automatically review and approve the pull request. The approval would then trigger the `automerger` GitHub Action which would merge the approved pull request. A proof-of-concept (PoC) pull request demonstrating the vulnerability was submitted with our permission. We subsequently reverted the PoC pull request, disabled and removed the `automerger` GitHub Action and disabled and removed the `review-cask-pr` GitHub Action from all vulnerable repositories.

What was impacted

The discovered vulnerability would allow an attacker to inject arbitrary code into a cask and have it be merged automatically. This is due to a flaw in the `git_diff` dependency of the `review-cask-pr` GitHub Action, which is used to parse a pull request's diff for inspection. Due to this flaw, the parser can be spoofed into completely ignoring the offending lines, resulting in successfully approving a malicious pull request.

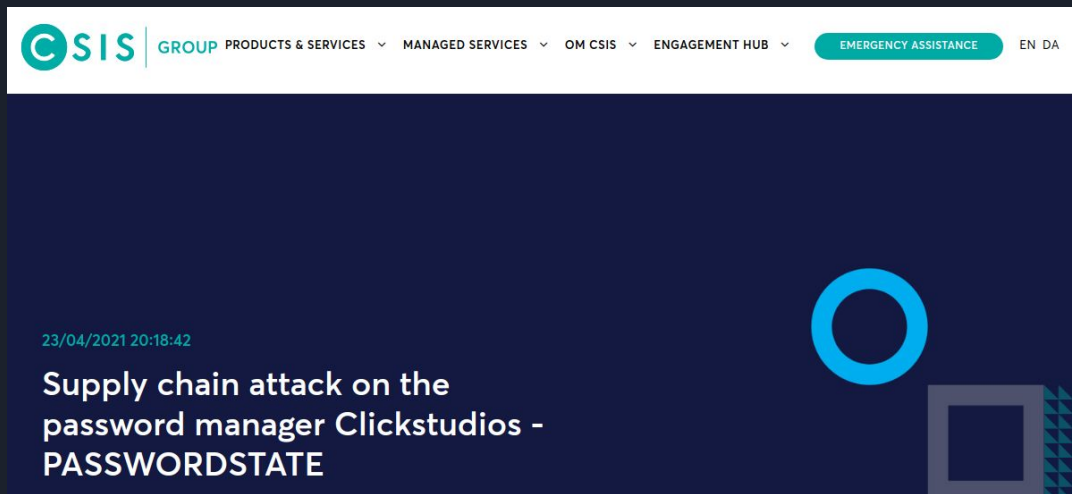
A single cask was compromised with a harmless change for the duration of the demonstration pull request until its reversal. No action is required by users due to this incident.





Clickstudios 23. apríl

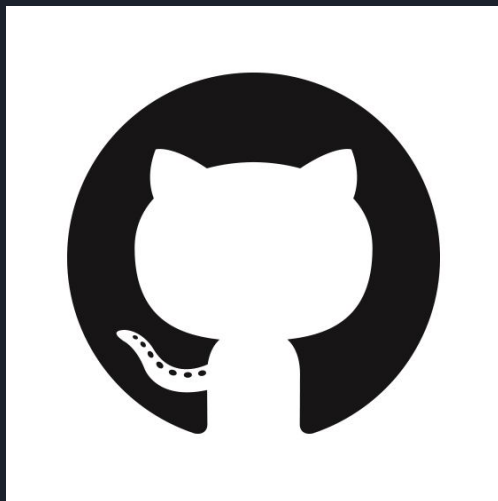
Seinnihluti apríl





GitHub 25. apríl

Seinnihluti apríl



Supply Chain Attacks via GitHub.com Releases

🕒 April 25, 2021 👤 nightwatchcyber 📁 Advisories, Research 🔗 [github, supplychainattack](#)

Summary

Release functionality on [GitHub.com](#) allows modification of assets within a release by any project collaborator. This can occur after the release is published, and without notification or audit logging accessible in the UI to either the project owners or the public. However, some audit information may be available via the GitHub APIs. An attacker can compromise a collaborator's account and use it to modify releases without the knowledge of project owners or the public, thus resulting in supply chain attacks against the users of the project.

This issue was reported to the vendor – their response is that this is intended behavior and is an intentional design decision. While the vendor is planning improvements in this area, they are not able to provide additional details. GitHub.com paid plans and the GitHub enterprise server were not tested.



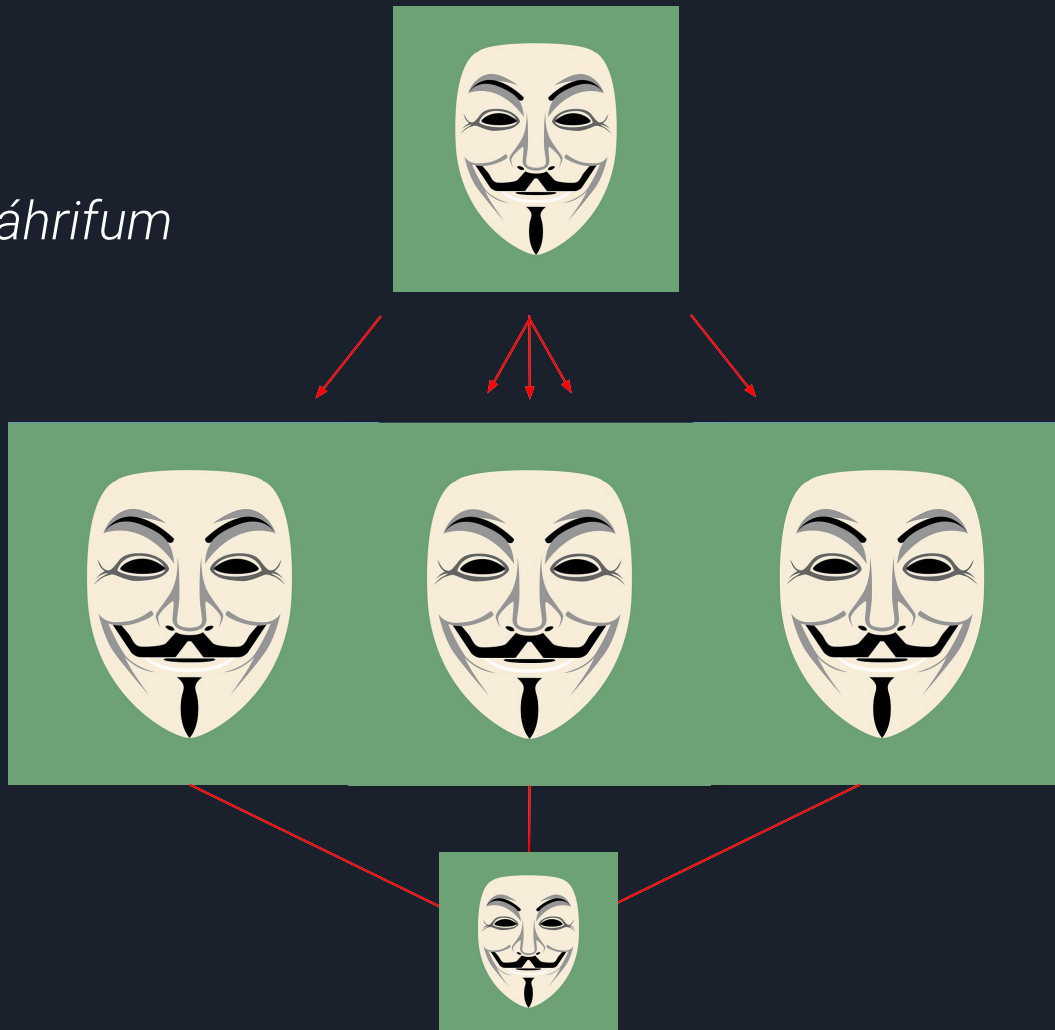
Miklu, miklu fleiri fyrir áhrifum





Keðjuverkun

Miklu, miklu fleiri fyrir áhrifum





Flugvélar

Miklu, miklu fleiri fyrir áhrifum





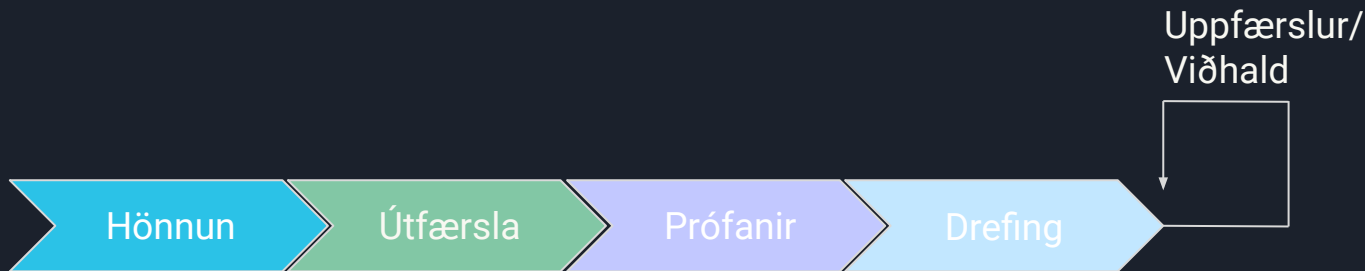
Hver er okkar birgðakeðja?





Skilgreining

- Hvað er skilgreint sem birgðakeðja?
 - Allir hlutar sem koma við þróun á vöru fyrirtækja
 - Hvernig er þróun hugbúnaðar?
 - Hvaða tól erum við að nota þar?





Stafar samt í alvöru
hætta af þessu?

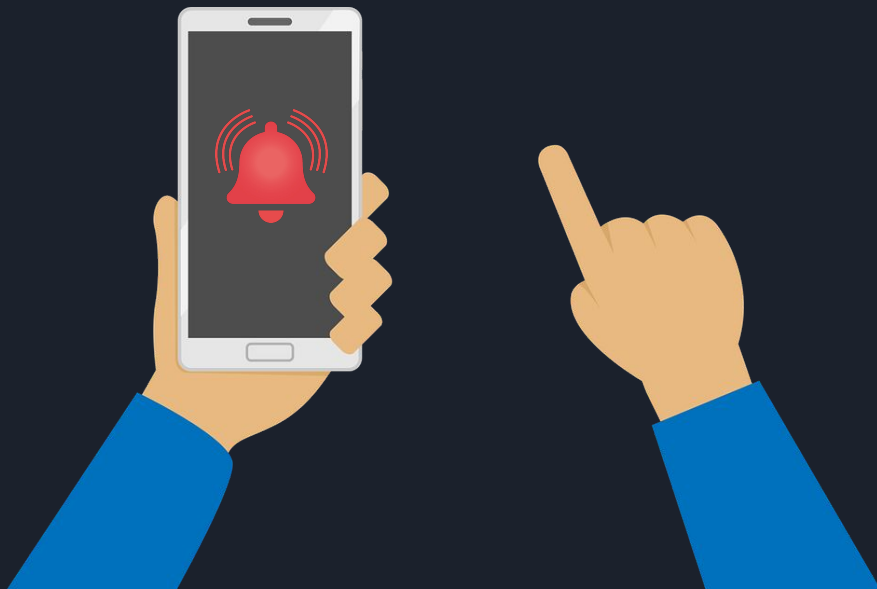




Mánalogn

Stafar samt í alvöru hættu af þessu?

- Fyrirtæki sem sér um að fylgjast með innranetum viðskiptavina
 - Sendir þér tilkynningu beint í símann!





Hönnun

Stafar samt í alvöru hættu af þessu?



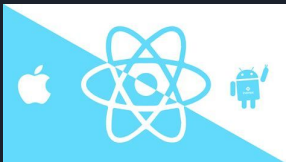
django

Bakendi



django

Bakendi



Framendi





Útfærslur

Stafar samt í alvöru hættu af þessu?





Prófanir

Stafar samt í alvöru hættu af þessu?





Dreifing

Stafar samt í alvöru hætta af þessu?





Uppfærslur og viðhald

Stafar samt í alvöru hættu af þessu?

- SolarWinds
 - Árás í gegnum uppfærslu
- 33,000 viðskiptavinir
 - 18,000 náðu í óværu (*malware*)
 - Hundruðir fyrir miðaðri árás





Uppfærslur og viðhald

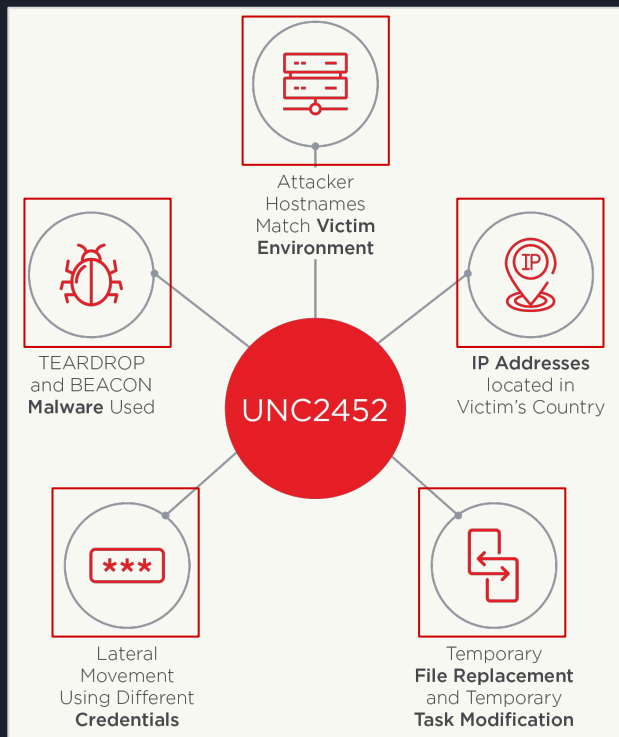
Stafar samt í alvöru hættu af þessu?





Uppfærslur og viðhald

Stafar samt í alvöru hættu af þessu?



Samantekt

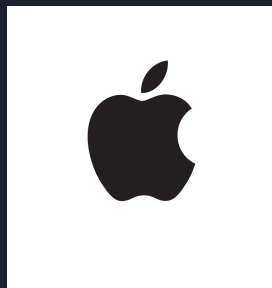
- *Supply Chain Attacks*
 - Tímabært umræðuefni
 - *Dependency Confusion*
 - Apríl atvik
 - Keðjuverkun
- Mánaðlogn
 - Hættur í Þróunarferlinu
- SolarWinds
 - SUNBURST bakdyr



Fórnalömb



Microsoft



Uber

NETFLIX

