HashiCorp is the latest victim of Codecov supply-chain attack

bleepingcomputer.com/news/security/hashicorp-is-the-latest-victim-of-codecov-supply-chain-attack/

Ax Sharma

By
Ax Sharma

- April 24, 2021
- 02:16 AM
- 0

Open-source software tools and Vault maker HashiCorp has disclosed a security incident that occurred due to the recent Codecov attack.

HashiCorp, a Codecov customer, has stated that the recent Codecov supply-chain attack aimed at collecting developer credentials led to the exposure of HashiCorp's GPG signing key.

The private key is used by HashiCorp to sign and verify software releases, and has since been rotated as a precaution.

HashiCorp discloses code-signing key compromise

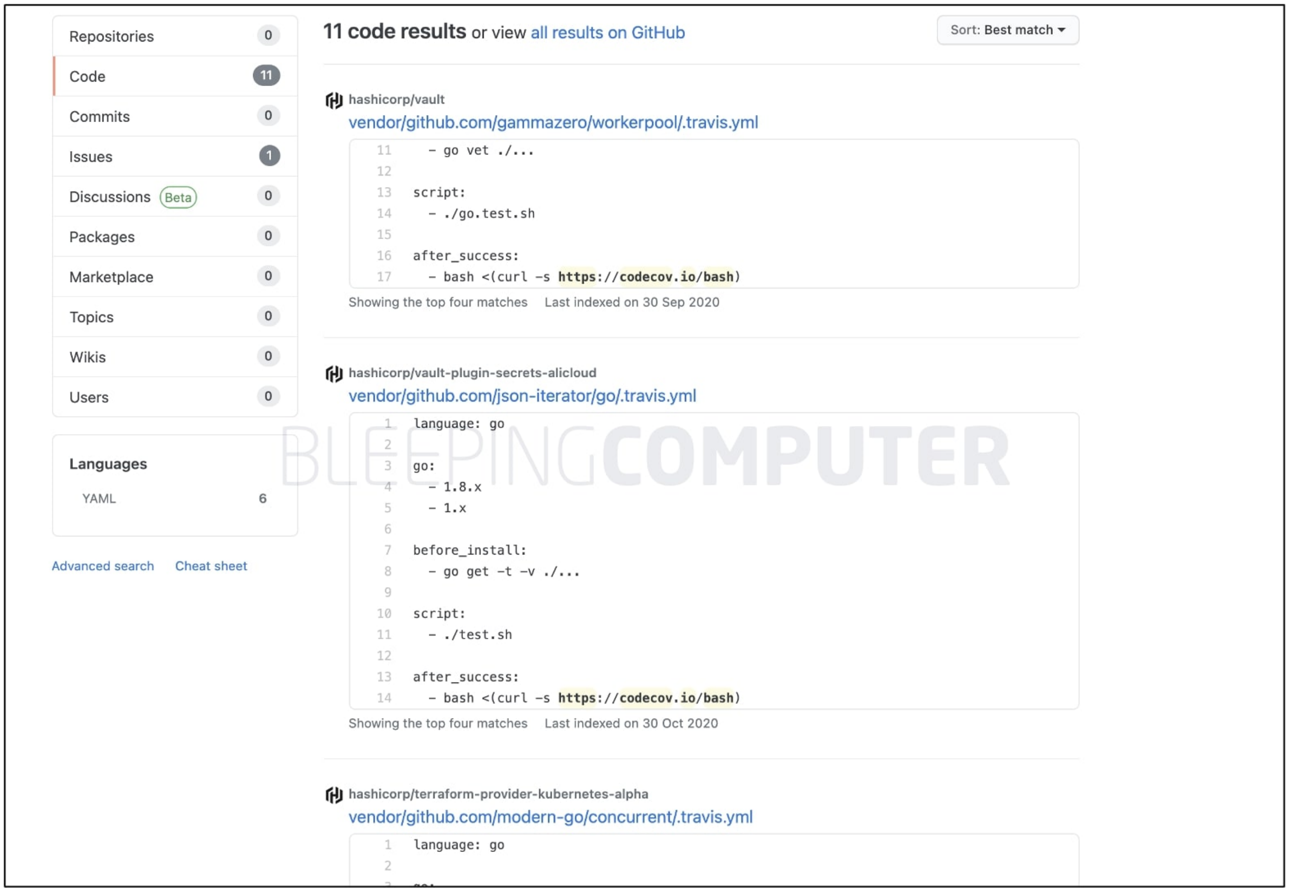
This week, HashiCorp, a notable open-source software tools and infrastructure provider, disclosed that the recent Codecov supply-chain attack had impacted a subset of their Continuous Integration (CI) pipelines.

The company states that as a result of this, the GPG key used by HashiCorp to sign and verify software releases was exposed.

Codecov provides software testing and code coverage services to over 29,000 customers.

On April 1st, Codecov had learned that due to a flaw in their Docker image, threat actors had obtained credentials to the Bash Uploader scripts used by their customers.

The Bash Uploaders were modified with a malicious line of code that exfiltrated environment variables and secrets collected from some customers' CI/CD environments, to an attacker-controlled server.



11 code results or view all results on GitHub

hashicorp/vault
vendor/github.com/gammazero/workerpool/.travis.yml

```
  - go vet ./...

script:
  - ./go.test.sh

after_success:
  - bash <(curl -s https://codecov.io/bash)
```

Showing the top four matches Last indexed on 30 Sep 2020

hashicorp/vault-plugin-secrets-alicloud
vendor/github.com/json-iterator/go/.travis.yml

```
language: go

go:
  - 1.8.x
  - 1.x

before_install:
  - go get -t -v ./...

script:
  - ./test.sh

after_success:
  - bash <(curl -s https://codecov.io/bash)
```

Showing the top four matches Last indexed on 30 Oct 2020

hashicorp/terraform-provider-kubernetes-alpha
vendor/github.com/modern-go/concurrent/.travis.yml

```
language: go

```

Instances of Codecov Bash Uploader used in HashiCorp code
According to Codecov's investigation, the initial compromise of the Bash Uploader happened on January 31, making this attack last around two months.

In all this, HashiCorp's GPG private keythat signs hashes used to verify HashiCorp's product downloads was exposed.

"While investigation has not revealed evidence of unauthorized usage of the exposed GPG key, it has been rotated in order to maintain a trusted signing mechanism."

A new GPG keypair (fingerprint shown below) has been published that is to be used from now on:

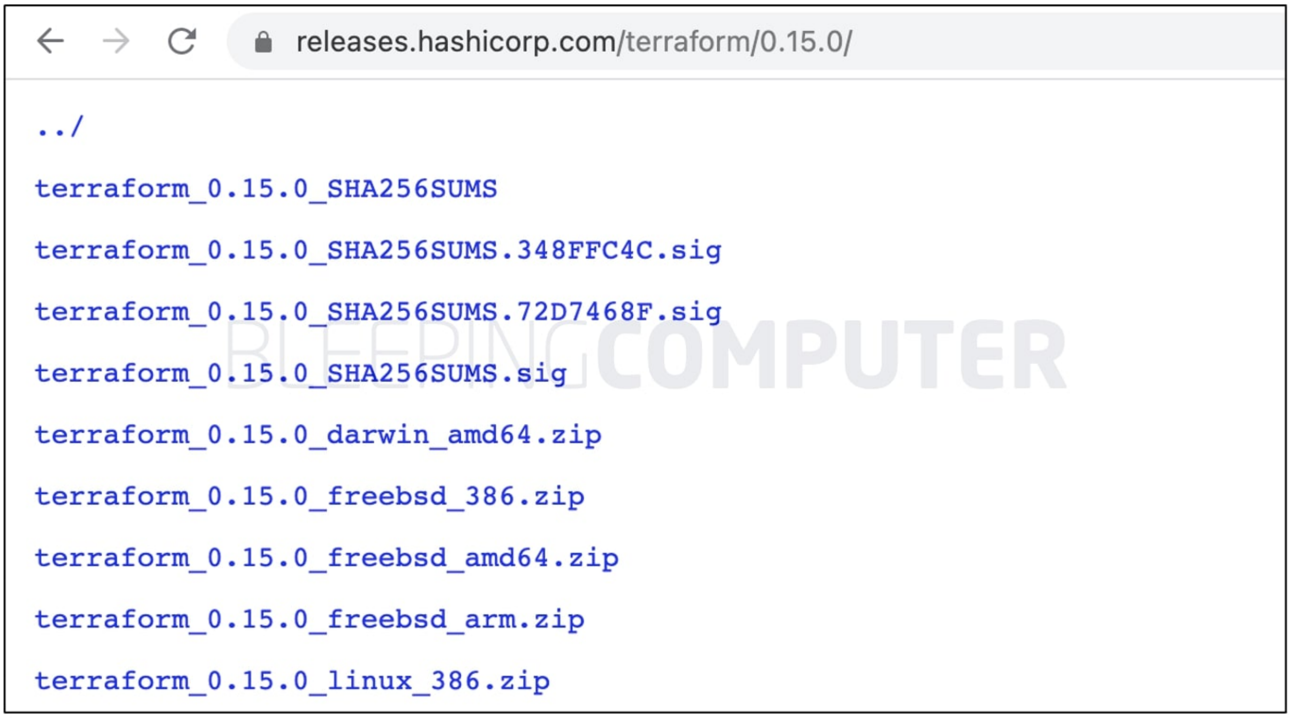
C874 011F 0AB4 0511 0D02 1055 3436 5D94 72D7 468F

The older, compromised GPG keypair (fingerprint shown below) has been revoked:

91A6 E7F8 5D05 C656 30BE F189 5185 2D87 348F FC4C

"Existing releases have been validated and re-signed," states HashiCorp in a security event disclosure.

According to HashiCorp, this incident has only impacted HashiCorp's SHA256SUM signing mechanism.



```
../
terraform_0.15.0_SHA256SUMS
terraform_0.15.0_SHA256SUMS.348FFC4C.sig
terraform_0.15.0_SHA256SUMS.72D7468F.sig
terraform_0.15.0_SHA256SUMS.sig
terraform_0.15.0_darwin_amd64.zip
terraform_0.15.0_freebsd_386.zip
terraform_0.15.0_freebsd_amd64.zip
terraform_0.15.0_freebsd_arm.zip
terraform_0.15.0_linux_386.zip
```

Example SHA256SUM files provided with HashiCorp releases

MacOS code signing (notarization), as well as, Windows AuthentiCode signing of HashiCorp releases, has not been affected by the exposed private key.

Likewise, signing for Linux packages (Debian and RPM) available on releases.hashicorp.com remains unaffected.

HashiCorp's Terraform yet to be patched

However, HashiCorp's advisory does state that their Terraform product is yet to be patched to use the new GPG key.

Terraform is an open-source infrastructure-as-code software tool used for safely and predictably creating, changing, and improving infrastructure.

"Terraform automatically downloads provider binaries during the `terraform init` operation and performs signature verification during this process," states Jamie Finnigan, HashiCorp's Director of Product security.

The company states that patched releases of Terraform and related tools will be published that use the new GPG key during automatic code verification.

"In the short term, transport-level TLS protects official Terraform provider binaries downloaded during `init`, and manual verification of Terraform and its providers can be performed with the new key and signatures as described at https://hashicorp.com/security," continues Finnigan in the security advisory.

As a part of its incident response activities, HashiCorp is further investigating if any other information was exposed from the Codecov incident and plans on providing relevant updates, as the investigation progresses.

As reported by BleepingComputer earlier this week, hundreds of Codecov customer networks were reportedly breached due to the Codecov Bash Uploader compromise.

U.S. federal investigators have also stepped in and are working with Codecov and their customers, to investigate the full impact of the attack.

As such, more security disclosures are expected to come out in the following weeks from different customers.

Software supply-chain attacks continue to be on the rise as they become the latest focus of threat actors.

Just yesterday, BleepingComputer reported that the Passwordstate enterprise password manager used by many Fortune 500 customers was hacked in a supply-chain attack.

Related Articles:

Hacker says hijacking libraries, stealing AWS keys was ethical research

Popular Python and PHP libraries hijacked to steal AWS keys

Check your gems: RubyGems fixes unauthorized package takeover bug

GitHub to require 2FA from active developers by the end of 2023

Open source 'Package Analysis' tool finds malicious npm, PyPI packages

- Bash
- Codecov
- Data Breach

- Developer
- Docker
- Supply Chain
- Supply-Chain Attack

Ax Sharma

Ax Sharma is a Security Researcher and Tech Reporter. His works and expert analyses have frequently been featured by leading media outlets including Fortune, Business Insider, The Register, TechRepublic, etc. Ax's expertise lies in vulnerability research, malware analysis, and open source software. He's an active community member of the OWASP Foundation, Open Source Security Foundation (OpenSSF), and the British Association of Journalists (BAJ). Send any tips via email or Twitter DM.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: