lookup Function Information Discolosure

Low **technosophos** published **GHSA-q8q8-93cv-v6h8** on Apr 22, 2020

Package

Helm

Affected versions	Patched versions
3.1.0-3.1.2	3.1.3, 3.2.0

Description

The Helm core maintainers have identified an information disclosure vulnerability in Helm 3.0.0-3.1.2.

Impact

`lookup` is a Helm template function introduced in Helm v3. It is able to lookup resources in the cluster to check for the existence of specific resources and get details about them. This can be used as part of the process to render templates.

The documented behavior of `helm template` states that it does not attach to a remote cluster. However, as the recently added `lookup` template function circumvents this restriction and connects to the cluster even during `helm template` and `helm install|update|delete|rollback --dry-run`. The user is not notified of this behavior.

Running `helm template` should not make calls to a cluster. This is different from `install`, which is presumed to have access to a cluster in order to load resources into Kubernetes. Helm 2 is unaffected by this vulnerability.

A malicious chart author could inject a `lookup` into a chart that, when rendered through `helm template`, performs unannounced lookups against the cluster a user's `KUBECONFIG` file points to. This information can then be disclosed via the output of `helm template`.

Patches

This issue has been fixed in Helm 3.2.0

Workarounds

Due to another bug (also fixed in Helm 3.2.0), the command `helm lint` will fail with an error if the `lookup` function is used in a chart. Therefore, run `helm lint` on an untrusted chart before running `helm template`.

Alternately, setting the `KUBECONFIG` environment variable to point to an empty Kubernetes configuration file will prevent unintended network connections.

Finally, a chart may be manually analyzed for the presence of a `lookup` function in any file in the `templates/` directory.

For more information

If you have any questions or comments about this advisory:

- Open an issue in the Helm repository
- For security-specific issues, email us at cncf-helm-security@lists.cncf.io

Severity

Low

CVE ID

CVE-2020-11013

Weaknesses

No CWEs