Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in spinnaker

Moderate jasonmcintosh published GHSA-34jx-3vmr-56v8 on Jan 3

Package

spinnaker

Affected versions	Patched versions
<1.26.7, <1.25.7, <1.24.7	1.26.7, 1.25.7, 1.24.7

Description

Impact

A path traversal vulnerability was discovered in uses of TAR files by AppEngine for deployments. This uses a utility to extract files locally for deployment without validating the paths in that deployment don't override system files. This would allow an attacker to override files on the container, POTENTIALLY introducing a MITM type attack vector by replacing libraries or injecting wrapper files.

Patches

Incoming...

Workarounds

Disable Google AppEngine deployments and/or disable artifacts that provide TARs.

References

To be updated. Reference examples:
https://bugzilla.redhat.com/show_bug.cgi?id=1584388

Code area (as of release 1.26):
https://github.com/spinnaker/clouddriver/blob/release-1.26.x/clouddriver-appengine/src/main/java/com/netflix/spinnaker/clouddriver/appengine/artifacts/ArtifactUtils.java

For more information

Email security@spinnaker.io

Severity

Moderate 6.6 / 10

CVSS base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

CVE ID

CVE-2021-39143

Weaknesses

CWE-22