Possible pod name collisions

High **minrk** published **GHSA-v7m9-9497-p9gr** on Jul 17, 2020

Package

jupyterhub-kubespawner (pypi)

Affected versions	Patched versions
<= 0.11.1	0.12

Description

Impact

What kind of vulnerability is it? Who is impacted?

JupyterHub deployments using:

- KubeSpawner <= 0.11.1 (e.g. zero-to-jupyterhub 0.9.0) and
- enabled named_servers (not default), and
- an Authenticator that allows:
  - usernames with hyphens or other characters that require escape (e.g. `user-hyphen` or `user@email`), and
  - usernames which may match other usernames up to but not including the escaped character (e.g. `user` in the above cases)

In this circumstance, certain usernames will be able to craft particular server names which will grant them access to the default server of other users who have matching usernames.

Patches

Has the problem been patched? What versions should users upgrade to?

Patch will be released in kubespawner 0.12 and zero-to-jupyterhub 0.9.1

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?

KubeSpawner

Specify configuration:

for KubeSpawner

```
from traitlets import default
from kubespawner import KubeSpawner

class PatchedKubeSpawner(KubeSpawner):
    @default("pod_name_template")
    def _default_pod_name_template(self):
        if self.name:
            return "jupyter-{username}-{servername}"
        else:
            return "jupyter-{username}"

    @default("pvc_name_template")
    def _default_pvc_name_template(self):
        if self.name:
            return "claim-{username}-{servername}"
        else:
            return "claim-{username}"

c.JupyterHub.spawner_class = PatchedKubeSpawner
```

Note for KubeSpawner: this configuration will behave differently before and after the upgrade, so will need to be removed when upgrading. Only apply this configuration while still using KubeSpawner ≤ 0.11.1 and remove it after upgrade to ensure consistent pod and pvc naming.

Changing the name template means pvcs for named servers will have different names. This will result in orphaned PVCs for named servers across Hub upgrade! This may appear as data loss for users, depending on configuration, but the orphaned PVCs will still be around and data can be migrated manually (or new PVCs created manually to reference existing PVs) before deleting the old PVCs and/or PVs.

References

Are there any links users can visit to find out more?

For more information

If you have any questions or comments about this advisory:

- Open an issue in kubespawner
- Email us at security@ipython.org

Credit: Jining Huang

Severity

High

CVE ID

CVE-2020-15110

Weaknesses

No CWEs