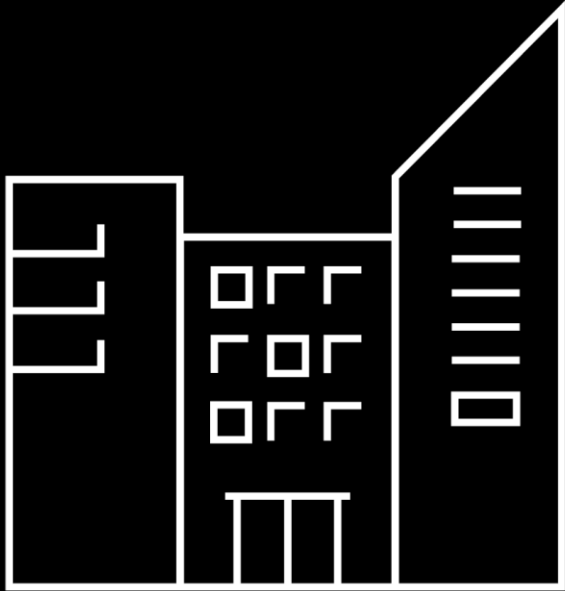




Automating Dependency Updates with Renovate

Tobias Gabriel, SAP Open Source Program Office
May 15th, 2024

PUBLIC

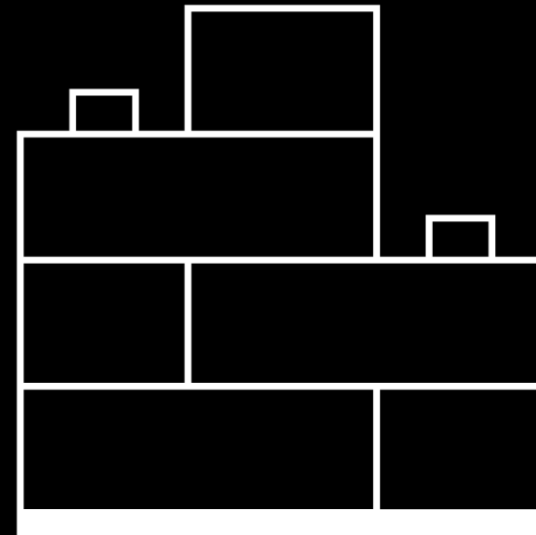


- Enterprise Software
- 40,000+ developers
- >1000 Enterprise Software products

- Senior Developer
- Open Source Program Office
- Improving Developer Experience

How many dependencies does SAP leverage?

20,000+



An iceberg floating in the ocean. The tip of the iceberg, which is above the water line, is labeled "Product Code". The much larger, submerged part of the iceberg, which is below the water line, is labeled "Dependencies". The water is a deep blue, and the sky is a light blue with some clouds.

Product Code

Dependencies

What even are dependencies?

```
34     - name: Use specified node version
35       uses: actions/setup-node@v1
36       with:
37         version: ${{ matrix.node_version }}
```

```
28     - ubuntu-latest
29     steps:
30     - uses: actions/checkout@v2
31       with:
```

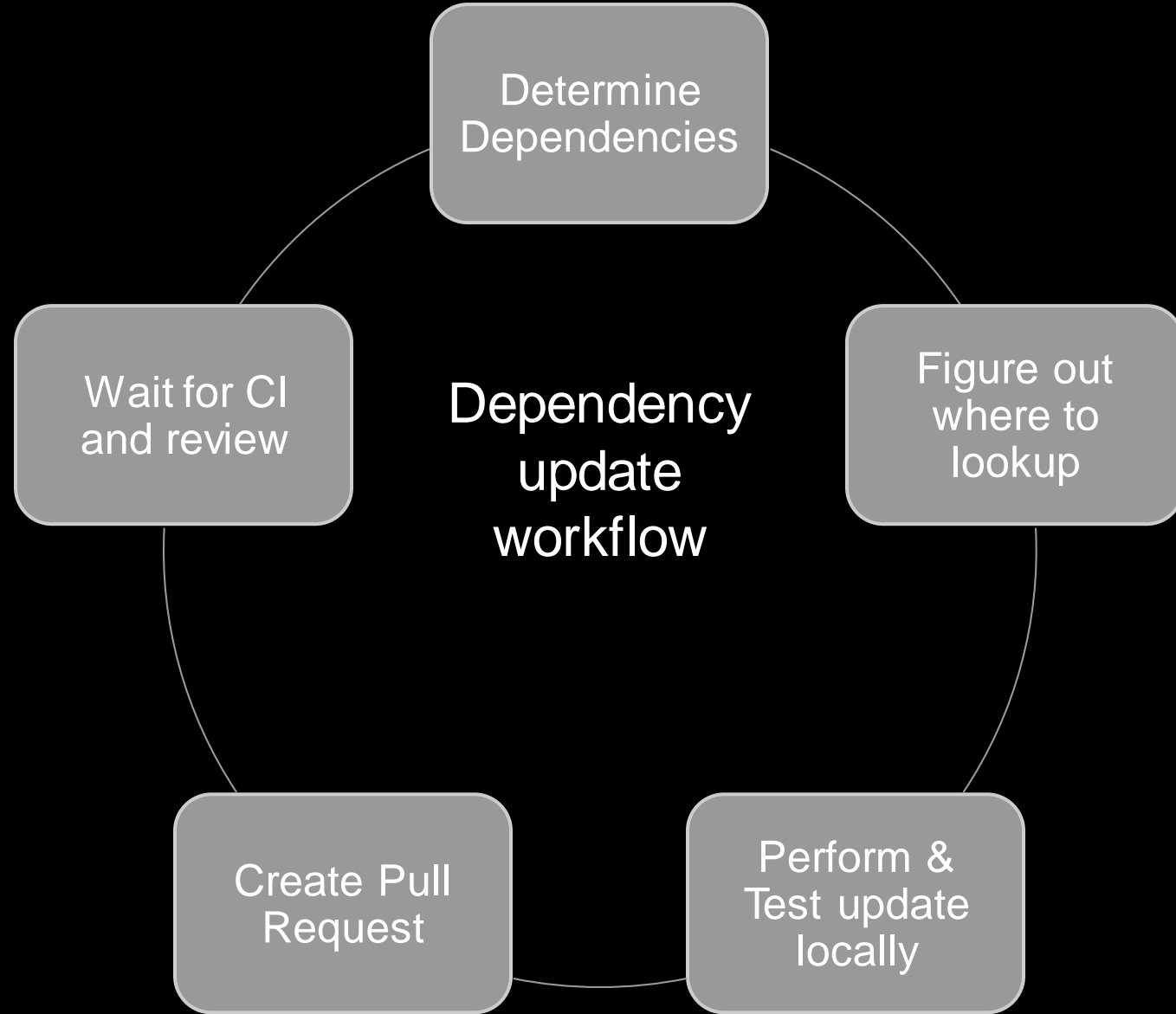
```
19     docs: https://github.com/eta-assistant/eta-assistant/issues ,
20     "contributors": [],
21     "dependencies": {
22       "@google-cloud/trace-agent": "^5.1.5",
23       "@octokit/auth-app": "^3.6.0",
24       "@octokit/plugin-retry": "^3.0.9",
25       "@octokit/plugin-throttling": "^3.5.2",
26       "@octokit/rest": "^18.10.0",
27       "async": "^3.2.1",
28       "body-parser": "^1.19.0",
29       "bunyan": "^1.8.15",
30       "bunyan-slack": "0.0.10",
31       "cls-rtracer": "^2.6.0",
32       "colors": "^1.4.0",
```

15 lines (9 sloc) | 261 Bytes

```
1 FROM node:16-alpine
```

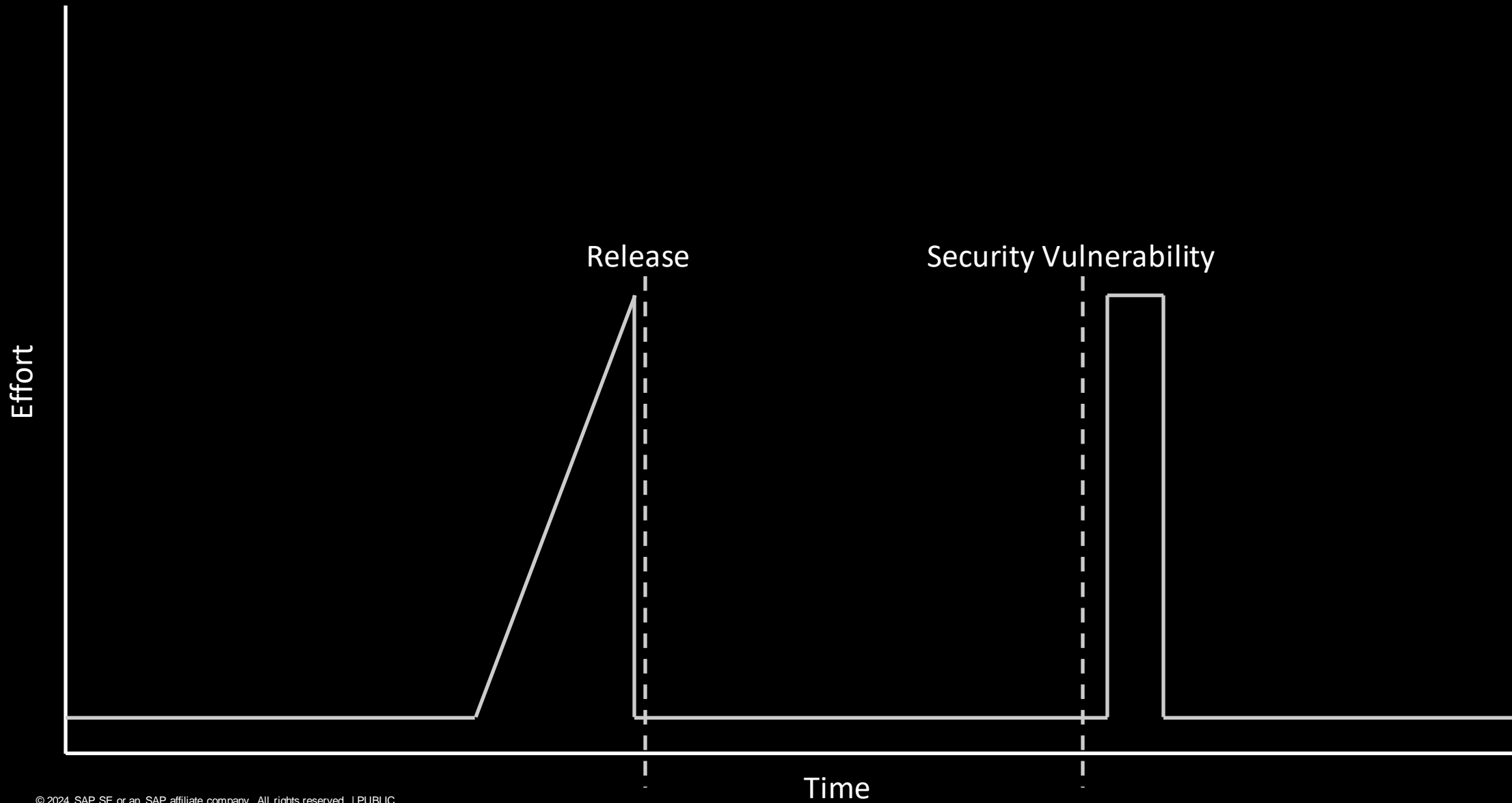
```
2
```

```
85     },
86     "engines": {
87       "node": "16",
88       "npm": "8"
89     },
```



**“...51% of developers agreed
that updating [dependencies]
was considered painful”**

2019 State of the Software Supply Chain Report, Sonatype



There is Automation



dependabot bot commented on behalf of github on 20 Jan 2021

Contributor  

Bumps [socket.io](#) from 2.2.0 to 2.4.0.

▶ Release notes

▶ Changelog

▶ Commits

 compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

▶ Dependabot commands and options

There is Automation



Update dependency typescript to v4.9.5 #9

Open ospo-renovate-... wants to merge 1 commit into `main` from `renovate/typescript-4.x`

Conversation **0** Commits **1** Checks **0** Files changed **2**

ospo-renovate-... bot commented on Mar 31, 2022 · edited ▾

This PR contains the following updates:

Package file	Type	Update	Change
package.json	devDependencies	minor	<code>4.5.5</code> -> <code>4.9.5</code>

Release Notes

► Microsoft/TypeScript (typescript)

Configuration

Schedule: Branch creation - At any time (no schedule defined), Automerge - At any time (no schedule defined).

Automerge: Disabled by config. Please merge this manually once you are satisfied.

Rebasing: Whenever PR becomes conflicted, or you tick the rebase/retry checkbox.

Ignore: Close this PR and you won't be reminded about this update again.

If you want to rebase/retry this PR, check this box

Advantages

chore(deps): update renovate/renovate docker tag to v37 #753

Merged

Tobias Gabriel merged 1 commit into `main` from `renovate/renovate-37.x` 4 days ago

Conversation 0 Commits 1 Checks 5 Files changed 1

ospo-renovate bot commented 12 days ago • edited

This PR contains the following updates:

Package	Type	Update	Change
renovate/renovate	final	major	36.107.0 -> 37.6.1

Release Notes

▶ renovatebot/renovate (renovate/renovate)

Eco

chore(deps): update dependency typescript to v5.2.2 #707

Merged

Tobias Gabriel merged 1 commit into `main` from `renovate/typescript-5.x` on Aug 28

Conversation 0 Commits 1 Checks 5 Files changed 2

ospo-renovate bot commented on Aug 26

This PR contains the following updates:

Package	Type	Update	Change
typescript (source)	devDependencies	minor	5.1.6 -> 5.2.2

Release Notes

▶ Microsoft/TypeScript (typescript)

Advantages

fix(deps): update dependency @sap/approuter to v8.6.1 #48

 Open

ospo-renovate wants to merge 1 commit into `main` from `renovate/sap-approuter-8.x` 

Conversation 0

Commits 1

Checks 0

Files changed 1



ospo-renovate bot commented on Feb 12, 2022 · edited ▾










This PR contains the following updates:

Package	Type	Update	Change
@sap/approuter	dependencies	minor	<code>8.5.0</code> -> <code>8.6.1</code>

Advantages

7 checks passed

- ✓  build (12, ubuntu-latest) build (12, ubuntu-latest)
- ✓  Analyze (javascript)
- ✓  Run deploy_gardener.yml Ansible playbook to c
- ✓  CodeQL No new or fixed alerts
- ✓  DeepScan 0 new and 0 fixed issues
- ✓  WIP Ready for review
- ✓  license/cla Contributor License Agreement is sig

ospo-rotate bot commented on 29 Jun 2021 · edited ·

Author

⚠ Artifact update problem

Renovate failed to update an artifact related to this branch. You probably do not want to merge this PR as-is.

🔄 Renovate will retry this branch, including artifacts, only when one of the following happens:

- any of the package files in this branch needs updating, or
- the branch becomes conflicted, or
- you click the rebase/retry checkbox if found above, or
- you rename this PR's title to start with "rebase!" to trigger it manually

The artifact failure details are included below:

File name: go.sum


```
Command failed: go get -d ./...
go: downloading github.wdf.sap.corp/devx-wing/logger-utils v1.2.0
go: downloading github.com/spf13/viper v1.8.0
go: downloading k8s.io/api v0.23.3
go: downloading k8s.io/apimachinery v0.23.3
go: downloading golang.org/x/crypto v0.0.0-20201002170205-7f63de1d35b0
go: downloading k8s.io/klog/v2 v2.30.0
go: downloading golang.org/x/net v0.0.0-20211209124913-491a49abca63
go: downloading golang.org/x/sys v0.0.0-20210831042530-f4d43177bf5e
go: downloading github.com/fsnotify/fsnotify v1.4.9
go: downloading github.com/mitchellh/mapstructure v1.4.1
go: downloading github.com/pelletier/go-toml v1.9.3
go: downloading github.com/spf13/cast v1.3.1
go: downloading gopkg.in/ini.v1 v1.62.0
go: downloading github.com/googleapis/gnostic v0.5.5
go: downloading k8s.io/utils v0.0.0-20211116205334-6203023598ed
go: downloading sigs.k8s.io/structured-merge-diff/v4 v4.2.1
go: downloading github.com/go-logr/logr v1.2.0
go: downloading golang.org/x/oauth2 v0.0.0-20210402161424-2e8d93401602
go: downloading gopkg.in/yaml.v3 v3.0.0-20210107192922-496545a6307b
go: downloading github.com/google/go-cmp v0.5.5
go: downloading sigs.k8s.io/json v0.0.0-20211020170558-c049b76a60c6
go: downloading github.com/json-iterator/go v1.1.12
go: downloading github.com/modern-go/reflect2 v1.0.2
github.wdf.sap.corp/devx-wing/healthchecker/client imports
    k8s.io/client-go/kubernetes imports
    k8s.io/client-go/kubernetes/typed/batch/v2alpha1 imports
    k8s.io/api/batch/v2alpha1: cannot find module providing package k8s.io/api/batch/v2alpha1
github.wdf.sap.corp/devx-wing/healthchecker/client imports
    k8s.io/client-go/kubernetes imports
    k8s.io/client-go/kubernetes/typed/discovery/v1alpha1 imports
    k8s.io/api/discovery/v1alpha1: cannot find module providing package k8s.io/api/discovery/v1alpha1
```

Cool things

Update dependency ws to v6.2.2 (SECURITY) #11

This PR contains the following updates:

Package	Type	Update	Change
node	engines	minor	18.17.1 -> 18.18.0
@types/node (source)	devDependencies	patch	18.17.17 -> 18.17.19
node	final	minor	18.17.1-slim -> 18.18.0-slim
node	stage	minor	18.17.1-slim -> 18.18.0-slim

 We found potential security issues

Some of the dependencies could be updated.

[Review vulnerable dependencies](#)

Only users who have been granted access can view this information.

[Dismiss](#)

Release Notes

▼ nodejs/node (node)

v18.18.0: 2023-09-18, Version 18.18.0 'Hydrogen' (LTS), @ruyadorno

[Compare Source](#)

Notable Changes

- [7dc731d4bf] - **build**: sync libuv header change (Jiawen Geng) #48078
- [490fc004b0] - **crypto**: update root certificates to NSS 3.93 (Node.js GitHub Bot) #49341
- [dd8cd97d4d] - **crypto**: update root certificates to NSS 3.90 (Node.js GitHub Bot) #48416
- [ea23870bec] - **deps**: add missing thread-common.c in uv.gyp (Santiago Gimeno) #48078
- [88855e0b1b] - **deps**: upgrade to libuv 1.46.0 (Santiago Gimeno) #48078
- [fb2b80fca0] - **deps**: upgrade to libuv 1.45.0 (Santiago Gimeno) #48078
- [249879e46c] - **doc**: add atlowChemi to collaborators (atlowChemi) #48757
- [89dc7bd6a] - **doc**: add ymeroz to collaborators (Vladimir Merozov) #48527

Workarounds

Cool things

2 .github/workflows/rules_pull-request.yml

Viewed ...

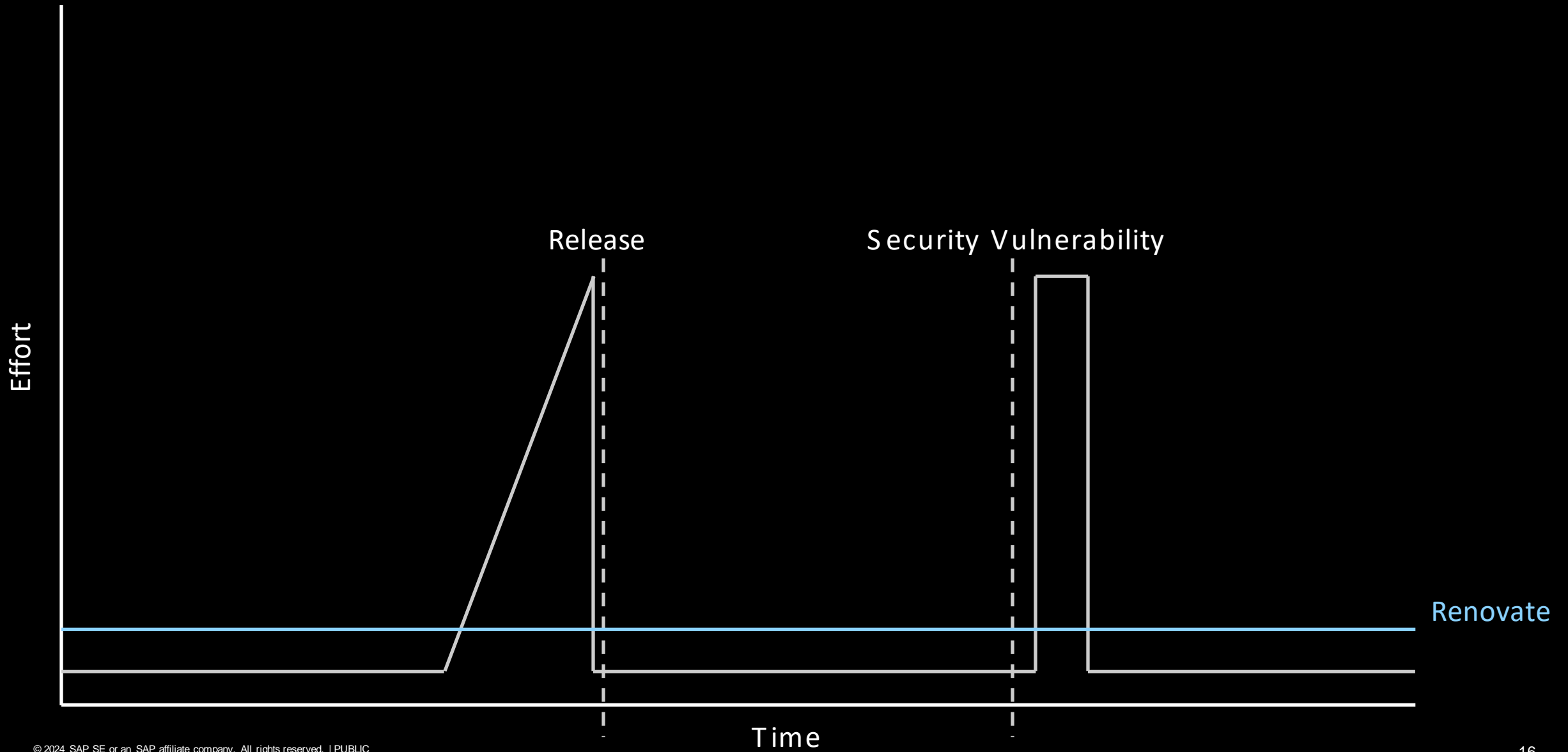
```
↑... @@ -18,7 +18,7 @@ jobs:
18 18     - uses: ghcom-actions/hashicorp-setup-terraform@v1
19 19       with:
20 20         # renovate: datasource=github-tags depName=hashicorp/terraform
21 21     - terraform_version: 1.0.6
21 21     + terraform_version: 1.1.0
22 22     - run: terraform init -backend-config="username=${{ secrets.ARTIFACTORY_USERNAME }}" -backend-config="password=${{ secrets.ARTIFACTORY_PASSWORD }}"
23 23     - name: Check format, if fails, format is violated. You can fix it locally with 'terraform fmt .'
24 24     run: terraform fmt -check -diff .
```

2 0_provider.tf

Viewed ...

```
↑... @@ -7,7 +7,7 @@ terraform {
7 7     subpath = "pagerduty"
8 8   }
9 9   +
10 10  -   required_version = "1.0.6"
10 10  +   required_version = "1.1.0"
11 11
12 12   required_providers {
13 13     pagerduty = {
```

↓...
↓



Nuking your CI system

70 Open ✓ 2 Closed

Update npm to v10
#73 opened 7 minutes ago by ospo-renovate 1 task

Update github/codeql-action action to v3
#72 opened 8 minutes ago by ospo-renovate 1 task

Update dependency webdriverio to v8
#71 opened 8 minutes ago by ospo-renovate 1 task

Update dependency supertest to v7
#70 opened 8 minutes ago by ospo-renovate 1 task

- CI can be easily overwhelmed
- Make sure to improve follow-up processes
- Do start small

Dependency definitions in Helm values

```
node:  
  image: "node"  
  tagVersion: "22.1.0"  
  customRegistry: registry.example.com
```



```
node:  
  repository: "node"  
  tag: "22.1.0"  
  registry: registry.example.com
```

Updatable via custom regex manager

Natively updatable

Standardized across all projects

Driving Adoption

Total PRs

432208

Merged PRs

329590

Open PRs

26466

Unmerged PRs

76152

Organizations

1163

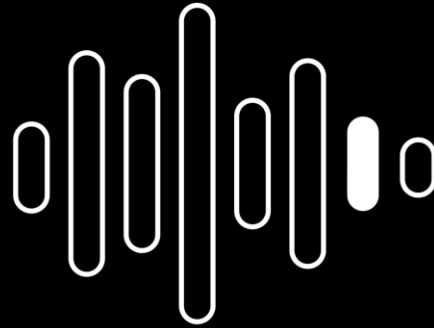
Repositories

16900

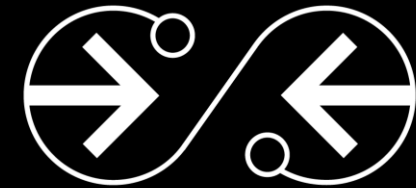
Our Lessons Learned



Leverage automation and tooling



Consider the whole development workflow



Continuously improve and be proactive

Thank you!

Contact information:

Tobias Gabriel

tobias.gabriel@sap.com



Learn more about Renovate at docs.renovatebot.com

