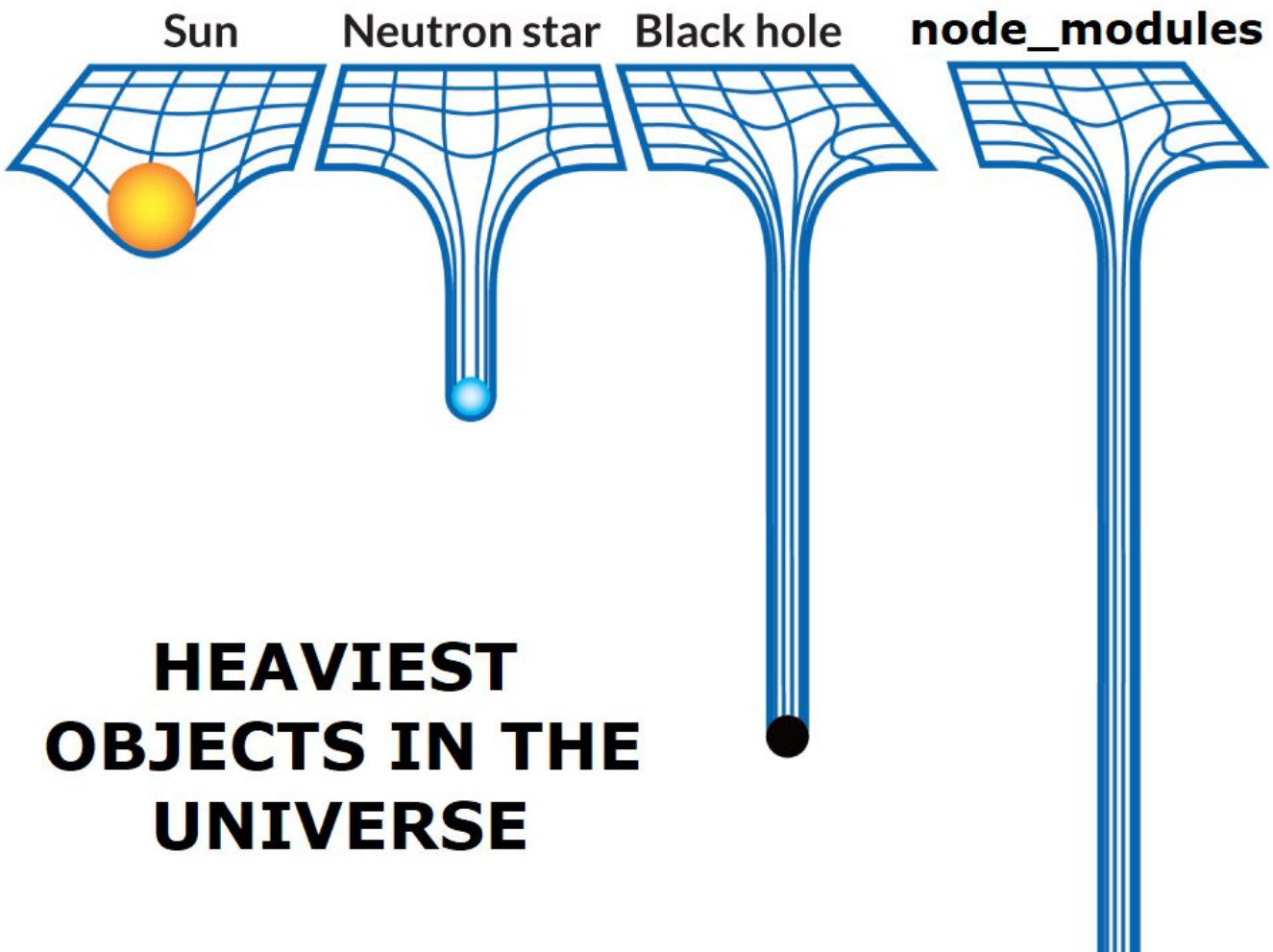
codecentric

Automatische Dependency Upgrades

Eine praxiserprobte Implementierung mit Dependabot



HEAVIEST OBJECTS IN THE UNIVERSE

15.7.0 (Oc

React

- Backport

15.6.2 (September

All Packages

- Switch from BSD + Pate

React DOM

- Fix a bug where modifyi
  #10032)
- CSS Columns are treate
- Fix bug in QtWebKit when wrapping synthetic events in proxies. (@walrusfruitcake in #10115)
- Prevent event handlers from receiving extra argument in development. (@aweary in #10115)
- Fix cases where `onChange` would not fire with `defaultChecked` on radio inputs. (@jquense in #10156)
- Add support for `controlList` attribute to allowed DOM properties (@nhunzaker in #9940)
- Fix a bug where creating an element with a ref in a constructor did not throw an error in development. (@iansu in #10025)

16.0.0 (September 26, 2017)

New JS Environment Requirements

- React 16 depends on the collection types Map and Set, as well as requestAnimationFrame. If you support older browsers and devices which may not yet provide these natively (e.g. <IE11), you may want to include a polyfill.

New Features

- Components can now return arrays and strings from `render`. (Docs coming soon!)
- Improved error handling with introduction of "error boundaries". Error boundaries are React components that catch JavaScript errors anywhere in their child component tree, log those errors, and display a fallback UI instead of the component tree that crashed.
- First-class support for declaratively rendering a subtree into another DOM node with `ReactDOM.createPortal()`. (Docs coming soon!)
- Streaming mode for server side rendering is enabled with `ReactDOMServer.renderToNodeStream()` and `ReactDOMServer.renderToStaticNodeStream()`. (@aickin in #10425, #10044, #10039, #10024, #9264, and others.)
- React DOM now allows passing non-standard attributes. (@nhunzaker in #10385, 10564, #10495 and others)

Breaking Changes

- There are several changes to the behavior of scheduling and lifecycle methods:
  - `ReactDOM.render()` and `ReactDOM.unstable_renderIntoContainer()` now return `null` if called from inside a lifecycle method.
    - To work around this, you can either use the new portal API or refs.
  - Minor changes to `setState` behavior:
    - Calling `setState` with null no longer triggers an update. This allows you to decide in an updater function if you want to re-render.

BSH Jira | Dashboards | Projects | Issues | Boards | More | Create | Search

Upgrade React to newest version

Edit | Add comment | Assign | More | New | Export

Details

Type:	Story	Resolution:	Unresolved
Priority:	Minor	Fix Version/s:	None
Affects Version/s:	None		
Component/s:	None		
Epic Link:	Architecture		

Description

Click to add description

Attachments

Drop files to attach, or browse.

People

Assignee:

Unassigned

Assign to me

Development

Create branch

Agile

Find on a board

Jigit Development

Click to load Git data

[redacted] added a comment

- 2024-02-02 8:08 AM - edited

Jann, Julius (codecentric) is this still needed??

Pin ·

[redacted] 10:11

Moin Julius,

ich hab hier irgendsoein SecurityVul Ticket vom SecuruityMgmr. bekommen das wir (so wie alle anderen Apps) lodash nutzen.

Ich bin mir ziemlich sicher das dass irrgendwo ein einer commonLib genutzt wird.

Hast du dir das zufaelligerweise mal angeschaut?

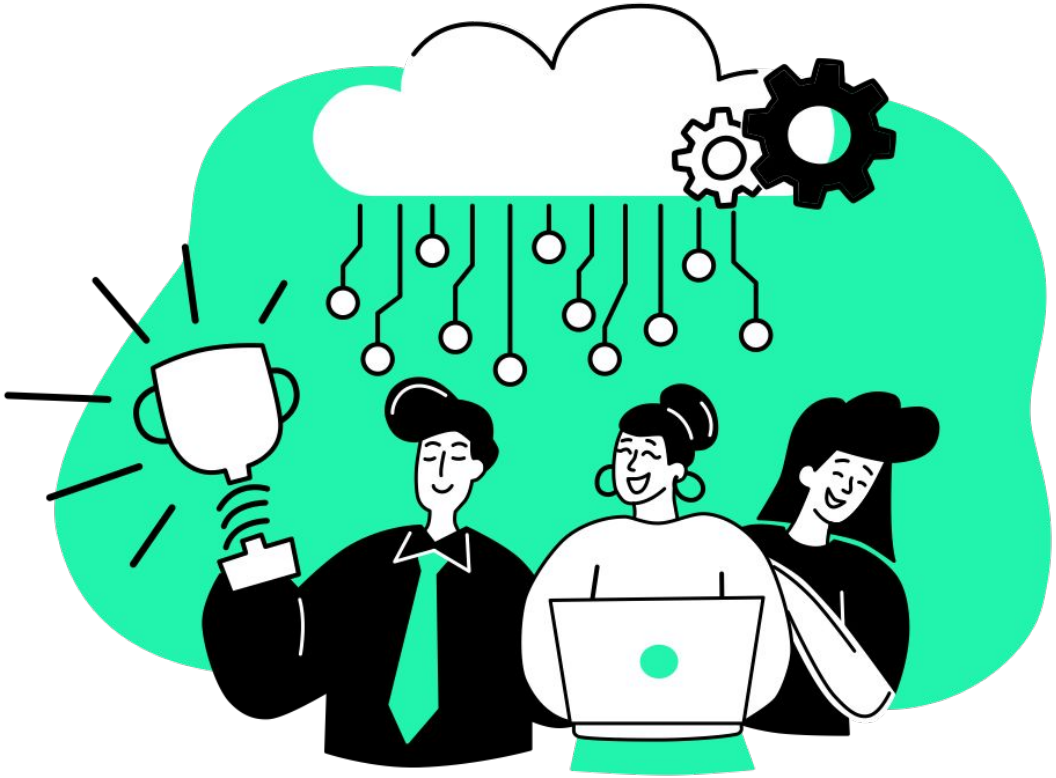
CVSS scores for CVE-2019-10744

Base Score	Base Severity	CVSS Vector	Exploitability Score
6.4	MEDIUM	AV:N/AC:L/Au:N/C:N/I:P/A:P	10.0
9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	3.9

NPM Update Party
09:30 bis 10:30

```
❯ yarn outdated
yarn outdated v1.22.22
info Color legend :
 "<red>"    : Major Update backward-incompatible updates
 "<yellow>" : Minor Update backward-compatible features
 "<green>"  : Patch Update backward-compatible bug fixes
```

Package	Current	Wanted	Latest	Package Type	URL
@babel/core	7.24.5	7.24.9	7.24.9	devDependencies	https://babel.dev/docs/en/next/babel-core
@babel/preset-env	7.24.5	7.24.8	7.24.8	devDependencies	https://babel.dev/docs/en/next/babel-preset-env
@babel/preset-typescript	7.24.1	7.24.7	7.24.7	devDependencies	https://babel.dev/docs/en/next/babel-preset-typescript
@hookform/resolvers	3.4.0	3.9.0	3.9.0	dependencies	https://react-hook-form.com
@react-native-async-storage/async-storage	1.23.1	1.24.0	1.24.0	devDependencies	https://github.com/react-native-async-storage/async-storage#readme
@react-native-community/datetimepicker	8.0.1	8.2.0	8.2.0	devDependencies	https://github.com/react-native-community/datetimepicker#readme
@react-navigation/bottom-tabs	6.5.20	6.6.1	6.6.1	dependencies	https://github.com/react-navigation/react-navigation#readme
@react-navigation/native	6.1.17	6.1.18	6.1.18	dependencies	https://reactnavigation.org
@react-navigation/stack	6.3.29	6.4.1	6.4.1	dependencies	https://reactnavigation.org/docs/stack-navigator/
@storybook/addon-actions	8.1.1	8.2.5	8.2.5	dependencies	https://github.com/storybookjs/storybook/tree/next/code/addons/actions
@storybook/addon-ondevice-actions	7.6.18	7.6.20	7.6.20	devDependencies	https://storybook.js.org/
@storybook/addon-ondevice-controls	7.6.18	7.6.20	7.6.20	devDependencies	https://github.com/storybookjs/react-native#readme
@storybook/react-native	7.6.18	7.6.20	7.6.20	devDependencies	https://storybook.js.org/
@testing-library/react-native	12.5.0	12.5.1	12.5.1	devDependencies	https://callstack.github.io/react-native-testing-library
@types/react	18.3.2	18.3.3	18.3.3	devDependencies	https://github.com/DefinitelyTyped/DefinitelyTyped/tree/master/types/react
@typescript-eslint/eslint-plugin	7.9.0	7.17.0	7.17.0	devDependencies	https://typescript-eslint.io/packages/eslint-plugin
@typescript-eslint/parser	7.9.0	7.17.0	7.17.0	devDependencies	https://typescript-eslint.io/packages/parser
eslint	8.57.0	8.57.0	9.7.0	devDependencies	https://eslint.org
eslint-plugin-jest	27.9.0	27.9.0	28.6.0	devDependencies	https://github.com/jest-community/eslint-plugin-jest#readme
eslint-plugin-prettier	5.1.3	5.2.1	5.2.1	devDependencies	https://github.com/prettier/eslint-plugin-prettier#readme



Julius Jann

julius.jann@codecentric.de
https://www.linkedin.com/in/julius-jann

Das Projekt

- Webshop Frontend
- TypeScript
- NextJS + GraphQL
- Vitest, React Testing Library, Playwright
- ArgoCD, HELM, Kubernetes
- GitHub

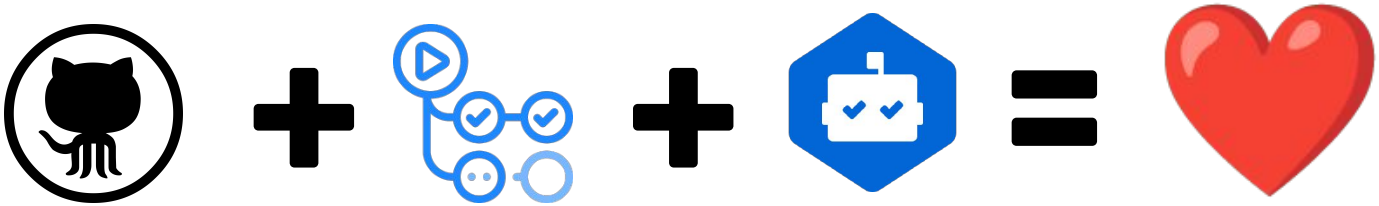
Security

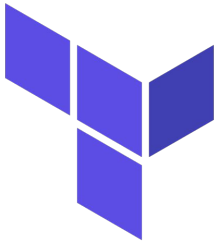
Speed

Developer Experience

Renovate

Dependabot





npm

yarn

Maven™

1 Open ✓ 14 Closed Package Ecosystem Manifest Severity Sort

ws affected by a DoS when handling a request with many HTTP headers High

#17 opened yesterday • Detected in ws (npm) • yarn.lock

Dependabot alerts / #8

Uncontrolled resource consumption in braces #8

Dismiss alert

Open · Opened last month on **braces** (npm) · yarn.lock

Upgrade braces to fix 1 Dependabot alert in yarn.lock

Upgrade braces to version `3.0.3` or later. For example:

```
braces@^3.0.3:
  version "3.0.3"
```

Create Dependabot security update

Package	Affected versions	Patched version
braces (npm)	< 3.0.3	3.0.3

The NPM package `braces` fails to limit the number of characters it can handle, which could lead to Memory Exhaustion. In `lib/parse.js`, if a malicious user sends "imbalanced braces" as input, the parsing will enter a loop, which will cause the program to start allocating heap memory without freeing it at any moment of the loop. Eventually, the JavaScript heap limit is reached, and the program will crash.

dependabot bot opened this last month

Severity

High 7.5 / 10

CVSS base metrics

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

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

Tags

Runtime dependency · Patch available

Weaknesses

CWE-400

CWE-1050

CVE ID

CVE-2024-4068

GHSA ID

GHSA-grv7-fg5c-xmjg

.github/dependabot.yaml

```yaml
version: 2
updates:
 - package-ecosystem: "npm"
   directory: "/"
   schedule:
     interval: "daily"
   open-pull-requests-limit: 100
   versioning-strategy: increase
```

.github/workflows/validate-pr.yaml

```yaml
name: Validate Pull Request

on:
 pull_request:

jobs:
 linter:
  # run linter

 tests:
  # run unit and integration tests

 browser-tests:
  # run browser tests

 build:
  # build the app
```

Bump eslint-plugin-prettier from 5.1.3 to 5.2.1 #27

Edit | Code

Open **dependabot** wants to merge 1 commit into `main` from `dependabot/npm_and_yarn/eslint-plugin-prettier-5.2.1`

Conversation 0 | Commits 1 | Checks 2 | Files changed 2 | +38 −13

dependabot bot commented on behalf of **github** yesterday

Bumps eslint-plugin-prettier from 5.1.3 to 5.2.1.

▶ Release notes

▶ Changelog

▶ Commits

compatibility 95%

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

`Bump eslint-plugin-prettier from 5.1.3 to 5.2.1` Verified ✓ e7a0de2

dependabot bot added the dependencies label yesterday

Add more commits by pushing to the **`dependabot/npm_and_yarn/eslint-plugin-prettier-5.2.1`** branch on **this repository**.

All checks have passed
4 successful checks
Show all checks

This branch has no conflicts with the base branch
Merging can be performed automatically.

Merge pull request | You can also open this in GitHub Desktop or view command line instructions.

Reviewers
Suggestions
Still in progress? Learn about draft PRs

Assignees
No one—assign yourself

Labels
dependencies

Projects
None yet

Milestone
No milestone

Development
Successfully merging this pull request may close these issues.
None yet

Notifications | Customize
Unsubscribe
You're receiving notifications because you're watching this repository.

0 participants

Lock conversation

- [ ] Bump react from 18.2.25 to 18.3.3 × dependencies
  #4 opened yesterday by dependabot bot
- [ ] Bump @types/react from 18.2.25 to 18.3.3 × dependencies
  #3 opened yesterday by dependabot bot
- [ ] Bump react-dom from 18.2.25 to 18.3.3 × dependencies
  #2 opened yesterday by dependabot bot
- [ ] Bump @types/react-dom from 18.2.25 to 18.3.3 × dependencies
  #1 opened yesterday by dependabot bot

.github/dependabot.yaml

```yaml
...

  groups:
   react:
     patterns:
       - "react"
       - "@types/react"
       - "react-dom"
       - "@types/react-dom"
```

.github/dependabot.yaml

```yaml
...

  groups:
   react:
     patterns:
       - "react*"
       - "@types/react*"
```

.github/dependabot.yaml

```yaml
...

  groups:
   react:
     patterns:
       - "react*"
       - "@types/react*"
```

.github/dependabot.yaml

```yaml
version: 2
updates:
 - package-ecosystem: "npm"
   directory: "/"
   schedule:
     interval: "daily"
   registries:
     - my-private-registry
   open-pull-requests-limit: 100
   versioning-strategy: increase
   groups:
     react:
       patterns:
         - "react*"
         - "@types/react*"

registries:
 my-private-registry:
   type: "npm-registry"
   url: "https://npm.pkg.github.com"
   # username doesn't matter
   username: any-username
   # must be added in the GitHub repo under Settings > Secrets and variables > Dependabot
   password: ${{ secrets.ACCESS-TOKEN }}
```

.github/workflows/validate-pr.yaml

```yaml
name: Validate Pull Request

on:
 pull_request:

permissions:
 contents: write
 pull-requests: write

jobs:

...
```

.github/workflows/validate-pr.yaml

```yaml
merge-dependabot:
 name: Auto-Merge Dependabot PR
 runs-on: ubuntu-latest
 if: ${{ github.actor == 'dependabot[bot]' }}
 needs:
   - linter
   - tests
   - browser-tests
   - build
 steps:
   - name: Auto-Merge
     run: gh pr merge --rebase "$PR_URL"
     env:
       PR_URL: ${{ github.event.pull_request.html_url }}
       GITHUB_TOKEN: ${{ secrets.GITHUB_TOKEN }}
```

.github/workflows/validate-pr.yaml

```yaml
merge-dependabot:
 ...

 steps:
   - name: Get Dependabot Metadata
     id: metadata
     uses: dependabot/fetch-metadata@v2
     with:
       github-token: ${{ secrets.GITHUB_TOKEN }}
   - name: Auto-Merge for Patch Upgrades
     if: ${{ steps.metadata.outputs.update-type == 'version-update:semver-patch' &&
             !contains(steps.metadata.outputs.dependency-names, '@do-not-merge') }}
     run: gh pr merge --rebase "$PR_URL"
     env:
       PR_URL: ${{ github.event.pull_request.html_url }}
       GITHUB_TOKEN: ${{ secrets.GITHUB_TOKEN }}
```

- Mit wenig Aufwand kann schon viel erreicht werden
- Probiert es einfach mal aus
- Nehmt Dependabot, wenn ihr GitHub nutzt
- Macht euch mit den Tools vertraut
- Entwickelt ein Gefühl für eure Dependencies
- Automatisiert nur, womit ihr euch wohl fühlt
- Prüft kritische Dependencies manuell
- Jeder Zwischenschritt bringt für sich schon Mehrwert

Julius Jann

julius.jann@codecentric.de
https://www.linkedin.com/in/julius-jann

Feedback

jann-cc commented now
@dependabot rebase
1

bshgroup / **blueprint-next-app**

Type / to search

Code | Issues | Pull requests 8 | Actions | Projects | Wiki | Security 1 | **Insights** | Settings

- Pulse
- Contributors
- Community
- Traffic
- Commits
- Code frequency
- Dependency graph
- Network
- Forks

Dependency graph

Dependencies | Dependents | Dependabot

Export SBOM

package.json ···

Recent update jobs

Dependabot version updates automatically keep your application up-to-date by periodically updating dependencies to their latest versions. Dependabot security updates can also help keep dependencies updated.

.github/workflows/validate-pr.yaml

```yaml
name: Validate Pull Request

on:
 pull_request:

permissions:
 contents: write
 pull-requests: write

jobs:
 linter:
   # run linter

 tests:
   # run unit and integration tests

 browser-tests:
   # run browser tests

 build:
   # build the app

 merge-dependabot:
   name: Auto-Merge Dependabot PRs
   runs-on: ubuntu-latest
   if: ${{ github.actor == 'dependabot[bot]' }}
   needs:
     - linter
     - tests
     - browser-tests
     - build
   steps:
     - name: Auto-Merge for Patch Upgrades
       run: gh pr merge --rebase "$PR_URL"
       env:
         PR_URL: ${{ github.event.pull_request.html_url }}
         GITHUB_TOKEN: ${{ secrets.GITHUB_TOKEN }}
```

.github/dependabot.yaml

```yaml
# Please see the documentation for all configuration options:
# https://docs.github.com/github/administering-a-repository/configuration-options-for-dependency-updates

version: 2
updates:
 - package-ecosystem: "npm"
   directory: "/"
   schedule:
     interval: "daily"
   registries:
     - my-private-registry
   open-pull-requests-limit: 100
   versioning-strategy: increase

   groups:
     react:
       patterns:
         - "react*"
         - "@types/react*"

registries:
 my-private-registry:
   type: "npm-registry"
   url: "https://npm.pkg.github.com"
   # username doesn't matter
   username: any-username
   # must be added in the GitHub repo under Settings > Secrets and variables > Dependabot
   password: ${{ secrets.ACCESS-TOKEN }}
```