

The project was successfully retested.

 keystone-classic 

master

 website/package.json 

Overview

History

Settings

Created Tue 22nd Feb 2022

Snapshot taken by snyk.io a few seconds ago

Retest now

IMPORTED BY

K

kiran.gopisetty@gmail.com

PROJECT OWNER

+

Add a project owner

ENVIRONMENT

+

Add a value

BUSINESS CRITICALITY

+

Add a value

LIFECYCLE STAGE

+

Add a value



ansi-html - Regular Expression Denial of Service (ReDoS)

SCORE
482

VULNERABILITY

CWE-400 

CVE-2021-23424 

CVSS 7.5 

HIGH

SNYK-JS-ANSIHTML-1296849 

Introduced through

gatsby@4.7.2

Exploit maturity

PROOF OF CONCEPT

Show less detail ^

Detailed paths

- Introduced through:** gatsby-starter-default@1.0.0 › gatsby@4.7.2 › @gatsbyjs/webpack-hot-middleware@2.25.2 › ansi-html@0.0.7
Fix: No remediation path available.
- Introduced through:** gatsby-starter-default@1.0.0 › gatsby@4.7.2 › @pmmmwh/react-refresh-webpack-plugin@0.4.3 › ansi-html@0.0.7
Fix: No remediation path available.

Overview

[ansi-html](#) is an An elegant lib that converts the chalked (ANSI) text to HTML.

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS). If an attacker provides a malicious string, it will get stuck processing the input for an extremely long time.

H ansi-regex - Regular Expression Denial of Service (ReDoS)

SCORE
482

VULNERABILITY | [CWE-400](#) | [CVE-2021-3807](#) | [CVSS 7.5](#) | **HIGH** | [SNYK-JS-ANSIREGEX-1583908](#)

Introduced through gatsby@4.7.2
Fixed in ansi-regex@6.0.1, @5.0.1
Exploit maturity **PROOF OF CONCEPT**

Show less detail ^

Detailed paths

- Introduced through: gatsby-starter-default@1.0.0 › gatsby@4.7.2 › gatsby-cli@4.7.0 › yurnalist@2.1.0 › strip-ansi@5.2.0 › ansi-regex@4.1.0
Fix: No remediation path available.

Overview

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) due to the sub-patterns `[[\\]()#;?]*` and `(?:;[-a-zA-Z\\d\\/#&.:=%@~_]*)*`.

C sanitize-html - Arbitrary Code Execution

SCORE
470

VULNERABILITY | [CWE-94](#) | [CVSS 9.4](#) | **CRITICAL** | [SNYK-JS-SANITIZEHTML-585892](#)

Introduced through gatsby-transformer-remark@4.11.0

Fixed in sanitize-html@2.0.0-beta

Exploit maturity NO KNOWN EXPLOIT

Show less detail ^

Detailed paths

- Introduced through: gatsby-starter-default@1.0.0 › gatsby-transformer-remark@4.11.0 › sanitize-html@1.27.5

Fix: No remediation path available.

Overview

[sanitize-html](#) is a library that allows you to clean up user-submitted HTML, preserving whitelisted elements and whitelisted attributes on a per-element basis

Affected versions of this package are vulnerable to Arbitrary Code Execution. Tag transformations which turn an attribute value into a text node using `transformTags` could be vulnerable to code execution.

 Ignore

unset-value - Prototype Pollution

VULNERABILITY | [CWE-1321](#) | [CVSS 7.5](#) | HIGH | [SNYK-JS-UNSETVALUE-2400660](#)

SCORE
446

Introduced through gatsby@4.7.2

Fixed in unset-value@2.0.1

Exploit maturity NO KNOWN EXPLOIT

Show less detail ^


Detailed paths

- **Introduced through:** gatsby-starter-default@1.0.0 › gatsby@4.7.2 › react-dev-utils@11.0.4 › fork-ts-checker-webpack-plugin@4.1.6 › micromatch@3.1.10 › snapdragon@0.8.2 › base@0.11.2 › cache-base@1.0.1 › unset-value@1.0.0
Fix: No remediation path available.
- **Introduced through:** gatsby-starter-default@1.0.0 › gatsby@4.7.2 › react-dev-utils@11.0.4 › fork-ts-checker-webpack-plugin@4.1.6 › micromatch@3.1.10 › braces@2.3.2 › snapdragon@0.8.2 › base@0.11.2 › cache-base@1.0.1 › unset-value@1.0.0
Fix: No remediation path available.
- **Introduced through:** gatsby-starter-default@1.0.0 › gatsby@4.7.2 › react-dev-utils@11.0.4 › fork-ts-checker-webpack-plugin@4.1.6 › micromatch@3.1.10 › extglob@2.0.4 › snapdragon@0.8.2 › base@0.11.2 › cache-base@1.0.1 › unset-value@1.0.0
Fix: No remediation path available.

...and 2 more

Overview

Affected versions of this package are vulnerable to Prototype Pollution via the `unset` function in `index.js`, because it allows access to object prototype properties.

NEW  [Learn about this type of vulnerability](#)

 Ignore

M

sanitize-html - Validation Bypass

SCORE

432

VULNERABILITY

|

CWE-20 

|

CVE-2021-26540 

|

CVSS 6.5 

|

MEDIUM

|

SNYK-JS-SANITIZEHTML-1070780 

Introduced through

gatsby-transformer-remark@4.11.0

Fixed in

sanitize-html@2.3.2

Exploit maturity

PROOF OF CONCEPT

Show less detail ^

Detailed paths

- **Introduced through:** gatsby-starter-default@1.0.0 › gatsby-transformer-remark@4.11.0 › sanitize-html@1.27.5

Fix: No remediation path available.

Overview

[sanitize-html](#) is a library that allows you to clean up user-submitted HTML, preserving whitelisted elements and whitelisted attributes on a per-element basis

Affected versions of this package are vulnerable to Validation Bypass. There is no proper validation of the hostnames set by the `allowedIframeHostnames` option when the `allowIframeRelativeUrls` is set to `true`. This allows attackers to bypass the hostname whitelist for the iframe element.

 Ignore

shell-quote - Remote Code Execution (RCE)

SCORE

405

VULNERABILITY | [CWE-94](#) | [CVE-2021-42740](#) | [CVSS 8.1](#) **HIGH** | [SNYK-JS-SHELLQUOTE-1766506](#)

Introduced through gatsby@4.7.2

Fixed in shell-quote@1.7.3

Exploit maturity NO KNOWN EXPLOIT

Show less detail ^

Detailed paths


- **Introduced through:** gatsby-starter-default@1.0.0 › gatsby@4.7.2 › react-dev-utils@11.0.4 › shell-quote@1.7.2

Fix: No remediation path available.

Overview

[shell-quote](#) is a package used to quote and parse shell commands.

Affected versions of this package are vulnerable to Remote Code Execution (RCE). An attacker can inject unescaped shell metacharacters through a regex designed to support Windows drive letters. If the output of this package is passed to a real shell as a quoted argument to a command with `exec()`, an attacker can inject arbitrary commands. This is because the Windows drive letter regex character class is `{A-z}` instead of the correct `{A-Za-z}`. Several shell metacharacters exist in the space between capital letter Z and lower case letter a, such as the backtick character.

 Ignore

immer - Prototype Pollution

SCORE

387

VULNERABILITY | [CWE-1321](#) | [CVE-2021-23436](#) | [CVSS 5.6](#) | MEDIUM | [SNYK-JS-IMMER-1540542](#)

Introduced through gatsby@4.7.2

Fixed in immer@9.0.6

Exploit maturity **PROOF OF CONCEPT**

Show less detail ^

Detailed paths

- Introduced through: gatsby-starter-default@1.0.0 › gatsby@4.7.2 › react-dev-utils@11.0.4 › immer@8.0.1
Fix: No remediation path available.

Overview

[immer](#) is a package that allows you to create your next immutable state by mutating the current one.

Affected versions of this package are vulnerable to Prototype Pollution. A type confusion vulnerability can lead to a bypass of CVE-2020-28477 when the user-provided keys used in the `path` parameter are arrays. In particular, this bypass is possible because the condition `(p === "__proto__" || p === "constructor")` in `applyPatches_` returns `false` if `p` is `['__proto__']` (or `['constructor']`). The `===` operator (strict equality operator) returns `false` if the operands have different type.

NEW

[Learn about this type of vulnerability](#)

 Ignore

M

browserslist - Regular Expression Denial of Service (ReDoS)

SCORE

372

VULNERABILITY

 | [CWE-400](#)  | [CVE-2021-23364](#)  | [CVSS 5.3](#)  |

MEDIUM

 | [SNYK-JS-BROWSERSLIST-1090194](#) 

Introduced through

gatsby@4.7.2

Fixed in

browserslist@4.16.5

Exploit maturity

PROOF OF CONCEPT

Show less detail



Detailed paths

- Introduced through: gatsby-starter-default@1.0.0 › gatsby@4.7.2 › react-dev-utils@11.0.4 › browserslist@4.14.2
- Fix: No remediation path available.

Overview

browserslist is a Share target browsers between different front-end tools, like Autoprefixer, Stylelint and babel-env-preset

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) during parsing of queries.

M

prompts - Regular Expression Denial of Service (ReDoS)

SCORE

372

VULNERABILITY

|

CWE-1333

|

CVE-2021-3868

|

CVSS 5.3

|

MEDIUM

|

SNYK-JS-PROMPTS-1729737

Introduced through	gatsby@4.7.2
Fixed in	prompts@2.4.2
Exploit maturity	PROOF OF CONCEPT

Show less detail ^

Detailed paths

- Introduced through: gatsby-starter-default@1.0.0 › gatsby@4.7.2 › react-dev-utils@11.0.4 › prompts@2.4.0
- Fix: No remediation path available.

Overview

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS). An attacker that is able to provide a crafted input to the strip functionality may cause an application to consume an excessive amount of CPU.

M

WS - Regular Expression Denial of Service (ReDoS)

SCORE

372

VULNERABILITY

|

CWE-400

|

CVE-2021-32640

|

CVSS 5.3

|

MEDIUM

|

SNYK-JS-WS-1296835

Introduced through gatsby@4.7.2

Fixed in ws@7.4.6, @6.2.2, @5.2.3

Exploit maturity **PROOF OF CONCEPT**

Show less detail ^

Detailed paths

- Introduced through: gatsby-starter-default@1.0.0 › gatsby@4.7.2 › eslint-plugin-graphql@4.0.0 › graphql-config@3.4.1 › @graphql-tools/url-loader@6.10.1 › ws@7.4.5
- Fix: No remediation path available.

Overview

`ws` is a simple to use websocket client, server and console for node.js.

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS). A specially crafted value of the `Sec-WebSocket-Protocol` header can be used to significantly slow down a `ws` server.

 Ignore

M node-fetch - Information Exposure

VULNERABILITY | [CWE-200](#) | [CVE-2022-0235](#) | [CVSS 6.5](#) | **MEDIUM** | [SNYK-JS-NODEFETCH-2342118](#)

SCORE
325

Introduced through gatsby-plugin-glamor@1.6.13 and gatsby@4.7.2

Fixed in node-fetch@2.6.7, @3.1.1

Exploit maturity **NO KNOWN EXPLOIT**

Show less detail ^


Detailed paths

- **Introduced through:** gatsby-starter-default@1.0.0 › gatsby-plugin-glamor@1.6.13 › glamor@2.20.40 › fbjs@0.8.18 › isomorphic-fetch@2.2.1 › node-fetch@1.7.3
Fix: No remediation path available.
- **Introduced through:** gatsby-starter-default@1.0.0 › gatsby@4.7.2 › eslint-plugin-graphql@4.0.0 › graphql-config@3.4.1 › @graphql-tools/url-loader@6.10.1 › cross-fetch@3.1.4 › node-fetch@2.6.1
Fix: No remediation path available.

Overview

`node-fetch` is a light-weight module that brings `window.fetch` to `node.js`

Affected versions of this package are vulnerable to Information Exposure when fetching a remote url with Cookie, if it get a `Location` response header, it will follow that url and try to fetch that url with provided cookie. This can lead to forwarding secure headers to 3th party.

 Ignore

M

sanitize-html - Access Restriction Bypass

SCORE
325

VULNERABILITY | [CWE-20](#) | [CVE-2021-26539](#) | [CVSS 6.5](#) | MEDIUM | [SNYK-JS-SANITIZEHTML-1070786](#)

Introduced through	gatsby-transformer-remark@4.11.0
Fixed in	sanitize-html@2.3.1
Exploit maturity	NO KNOWN EXPLOIT

Show less detail ^

Detailed paths

• **Introduced through:** gatsby-starter-default@1.0.0 › gatsby-transformer-remark@4.11.0 › sanitize-html@1.27.5

Fix: No remediation path available.

Overview

sanitize-html is a library that allows you to clean up user-submitted HTML, preserving whitelisted elements and whitelisted attributes on a per-element basis

Affected versions of this package are vulnerable to Access Restriction Bypass. Internationalized domain name (IDN) is not properly handled. This allows attackers to bypass hostname whitelist validation set by the allowedIframeHostnames option.

Ignore

M node-fetch - Denial of Service

SCORE
306

VULNERABILITY | CWE-400 | CVE-2020-15168 | CVSS 5.9 MEDIUM | SNYK-JS-NODEFETCH-674311

Introduced through	gatsby-plugin-glamor@1.6.13
Fixed in	node-fetch@2.6.1, @3.0.0-beta.9
Exploit maturity	NO KNOWN EXPLOIT

Show less detail ^

Detailed paths


• **Introduced through:** gatsby-starter-default@1.0.0 › gatsby-plugin-glamor@1.6.13 › glamor@2.20.40 › fbjs@0.8.18 › isomorphic-fetch@2.2.1 › node-fetch@1.7.3

Fix: No remediation path available.

Overview

node-fetch is a light-weight module that brings window.fetch to node.js

Affected versions of this package are vulnerable to Denial of Service. Node Fetch did not honor the `size` option after following a redirect, which means that when a content size was over the limit, a `FetchError` would never get thrown and the process would end without failure.

 Ignore