ghost

ghost@1.6.2

Source	CI/CLI
Created	20 hours ago
Taken by	CI/CLI v7.9.0
Hostname	iMac-CTA.local

Known vulnerabilities	**14**
Vulnerable paths	**108**
Dependencies	**595**

SHOW:

- (•) All vulnerabilities
- ( ) New vulnerabilities only

FILTER:

- [x] High severity (5)
- [ ] Medium severity (5)
- [ ] Low severity (4)
- [ ] Patched (0)
- [ ] Ignored (0)

High severity

New

Arbitrary Code Execution

Vulnerable module: **static-eval**

Introduced through: **jsonpath@0.2.12**

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › jsonpath@0.2.12 › static-eval@0.2.3
  Remediation: Upgrade to jsonpath@1.0.0.

Overview

`static-eval` **<https://www.npmjs.com/package/static-eval>** is a module to evaluate statically-analyzable expressions.

Affected versions of the package are vulnerable to Arbitrary Code Execution. If un-sanitized user input is passed to `static-eval`, it is possible to break out of the sandboxed instance, and execute arbitrary code from the standard library.

High severity

Prototype Override Protection Bypass

Vulnerable module: **qs**

Introduced through: **knex-migrator@2.1.5**, **sqlite3@3.1.8** and others

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › knex-migrator@2.1.5 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › request@2.76.0 › qs@6.3.0

Remediation: Your dependencies are out of date, otherwise you would be using a newer qs than qs@6.3.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › request@2.76.0 › qs@6.3.0

  Remediation: Your dependencies are out of date, otherwise you would be using a newer qs than qs@6.3.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › gscan@1.1.7 › express@4.14.0 › qs@6.2.0

  Remediation: Upgrade to gscan@1.2.1.

…and 1 more

Overview

`qs` **<https://www.npmjs.com/package/qs>** is a querystring parser that supports nesting and arrays, with a depth limit.

By default `qs` protects against attacks that attempt to overwrite an object's existing prototype properties, such as `toString()`, `hasOwnProperty()`,etc.

From `qs` **documentation <https://github.com/ljharb/qs>** :

By default parameters that would overwrite properties on the object prototype are ignored, if you wish to keep the data from those fields either use plainObjects as mentioned above, or set allowPrototypes to true which will allow user input to overwrite those properties. WARNING It is generally a bad idea to enable this option as it can cause problems when attempting to use the properties that have been overwritten. Always be careful with this option.

Overwriting these properties can impact application logic, potentially allowing attackers to work around security controls, modify data, make the application unstable and more.

In versions of the package affected by this vulnerability, it is possible to circumvent this protection and overwrite prototype properties and functions by prefixing the name of the parameter with `[` or `]`. e.g. `qs.parse("]=toString")` will return `{toString = true}`, as a result, calling `toString()` on the object will throw an exception.

Example:

```
qs.parse('toString=foo', { allowPrototypes: false })
            // {}

            qs.parse("]=toString", { allowPrototypes: false })
            // {toString = true} <== prototype overwritten
```

For more information, you can check out our blog **<https://snyk.io/blog/high-severity-vulnerability-qs/>** .

High severity

Regular Expression Denial of Service (ReDoS)

Vulnerable module: **timespan**

Introduced through: **knex-migrator@2.1.5**, **passport-ghost@2.3.1** and others

---

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › knex-migrator@2.1.5 › ghost-ignition@2.8.14 › bunyan-loggly@1.1.0 › loggly@1.1.1 › timespan@2.3.0
  Remediation: No remediation path available.
- *Introduced through*: ghost@1.6.2 › passport-ghost@2.3.1 › ghost-ignition@2.8.14 › bunyan-loggly@1.1.0 › loggly@1.1.1 › timespan@2.3.0
  Remediation: No remediation path available.
- *Introduced through*: ghost@1.6.2 › gscan@1.1.7 › ghost-ignition@2.8.14 › bunyan-loggly@1.1.0 › loggly@1.1.1 › timespan@2.3.0
  Remediation: No remediation path available.

…and 1 more

Overview

`timespan` **<https://www.npmjs.com/package/timespan>** is a JavaScript TimeSpan library for node.js (and soon the browser).

Affected versions of this package are vulnerable to Regular expression Denial of Service (ReDoS). It parses dates using regex strings, which may cause a slowdown of 10 seconds per 50k characters.

The Regular expression Denial of Service (ReDoS) is a type of Denial of Service attack. Many Regular Expression implementations may reach extreme situations that cause them to work very slowly (exponentially related to input size), allowing an attacker to exploit this and can cause the program to enter these extreme situations by using a specially crafted input and cause the service to excessively consume CPU, resulting in a Denial of Service.

You can read more about `Regular Expression Denial of Service (ReDoS)` on our **blog <https://snyk.io/blog/redos-and-catastrophic-backtracking/>** .

High severity

Regular Expression Denial of Service (ReDoS)

Vulnerable module: **fresh**

Introduced through: **brute-knex@2.0.0**, **gscan@1.1.7** and others

---

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › brute-knex@2.0.0 › express@4.14.0 › serve-static@1.11.2 › send@0.14.2 › fresh@0.3.0
  Remediation: Your dependencies are out of date, otherwise you would be using a newer fresh than fresh@0.3.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.
- *Introduced through*: ghost@1.6.2 › gscan@1.1.7 › express@4.14.0 › serve-static@1.11.2 › send@0.14.2 › fresh@0.3.0
  Remediation: Upgrade to gscan@1.2.1.

- *Introduced through*: ghost@1.6.2 › brute-knex@2.0.0 › express@4.14.0 › send@0.14.1 › fresh@0.3.0

  Remediation: Your dependencies are out of date, otherwise you would be using a newer fresh than fresh@0.3.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

…and 6 more

Overview

`fresh` **<https://www.npmjs.com/package/fresh>** is HTTP response freshness testing.

Affected versions of this package are vulnerable to Regular expression Denial of Service (ReDoS) attacks. A Regular Expression (`/ *, */`) was used for parsing HTTP headers and take about 2 seconds matching time for 50k characters.

The Regular expression Denial of Service (ReDoS) is a type of Denial of Service attack. Many Regular Expression implementations may reach extreme situations that cause them to work very slowly (exponentially related to input size), allowing an attacker to exploit this and can cause the program to enter these extreme situations by using a specially crafted input and cause the service to excessively consume CPU, resulting in a Denial of Service.

You can read more about `Regular Expression Denial of Service (ReDoS)` on our **blog <https://snyk.io/blog/redos-and-catastrophic-backtracking/>** .

High severity

Regular Expression Denial of Service (ReDoS)

Vulnerable module: **forwarded**

Introduced through: **brute-knex@2.0.0**, **gscan@1.1.7** and others

---

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › brute-knex@2.0.0 › express@4.14.0 › proxy-addr@1.1.5 › forwarded@0.1.0

  Remediation: Your dependencies are out of date, otherwise you would be using a newer forwarded than forwarded@0.1.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › gscan@1.1.7 › express@4.14.0 › proxy-addr@1.1.5 › forwarded@0.1.0

  Remediation: Your dependencies are out of date, otherwise you would be using a newer forwarded than forwarded@0.1.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › express@4.15.3 › proxy-addr@1.1.5 › forwarded@0.1.0

  Remediation: Your dependencies are out of date, otherwise you would be using a newer forwarded than forwarded@0.1.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

Overview

`forwarded` **<https://www.npmjs.com/package/forwarded>** is Parse HTTP X-Forwarded-For header.

Affected versions of this package are vulnerable to Regular expression Denial of Service (ReDoS) attacks. A Regular Expression (`/ *, */`) was used for parsing HTTP headers and take about 2 seconds matching time for 50k characters.

The Regular expression Denial of Service (ReDoS) is a type of Denial of Service attack. Many Regular Expression implementations may reach extreme situations that cause them to work very slowly (exponentially related to input size), allowing an attacker to exploit this and can cause the program to enter these extreme situations by using a specially crafted input and cause the service to excessively consume CPU, resulting in a Denial of Service.

You can read more about `Regular Expression Denial of Service (ReDoS)` on our **blog** **<https://snyk.io/blog/redos-and-catastrophic-backtracking/>** .

Medium severity

Regular Expression Denial of Service (ReDoS)

Vulnerable module: **tough-cookie**

Introduced through: **knex-migrator@2.1.5**, **sqlite3@3.1.8** and others

---

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › knex-migrator@2.1.5 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › request@2.76.0 › tough-cookie@2.3.2

  Remediation: Your dependencies are out of date, otherwise you would be using a newer tough-cookie than tough-cookie@2.3.2. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › request@2.76.0 › tough-cookie@2.3.2

  Remediation: Your dependencies are out of date, otherwise you would be using a newer tough-cookie than tough-cookie@2.3.2. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › knex-migrator@2.1.5 › ghost-ignition@2.8.14 › bunyan-loggly@1.1.0 › loggly@1.1.1 › request@2.75.0 › tough-cookie@2.3.2

  Remediation: Your dependencies are out of date, otherwise you would be using a newer tough-cookie than tough-cookie@2.3.2. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

…and 5 more

Overview

`tough-cookie` **<https://www.npmjs.com/package/tough-cookie>** is RFC6265 Cookies and Cookie Jar for node.js.

Affected versions of this package are vulnerable to Regular expression Denial of Service (ReDoS) attacks. An attacker may pass a specially crafted cookie, causing the server to hang.

The Regular expression Denial of Service (ReDoS) is a type of Denial of Service attack. Many Regular Expression implementations may reach extreme situations that cause them to work very slowly (exponentially related to input size), allowing an attacker to exploit this and can cause the program to enter these extreme situations by using a specially crafted input and cause the service to excessively consume CPU, resulting in a Denial of Service.

You can read more about `Regular Expression Denial of Service (ReDoS)` on our **blog** **<https://snyk.io/blog/redos-and-catastrophic-backtracking/>** .

Medium severity

Regular Expression Denial of Service (ReDoS)

Vulnerable module: **string**

Introduced through: **markdown-it-named-headers@0.0.4**

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › markdown-it-named-headers@0.0.4 › string@3.3.3

  Remediation: No remediation path available.

Overview

`string` **<https://www.npmjs.com/package/string>** is a JavaScript library for extra String methods.

Affected versions of this package are vulnerable to Regular expression Denial of Service (ReDoS). It uses regex in the `underscore` and `unescapeHTML` methods, which can cause a

slowdown of 2 seconds 50k characters.

The Regular expression Denial of Service (ReDoS) is a type of Denial of Service attack. Many Regular Expression implementations may reach extreme situations that cause them to work very slowly (exponentially related to input size), allowing an attacker to exploit this and can cause the program to enter these extreme situations by using a specially crafted input and cause the service to excessively consume CPU, resulting in a Denial of Service.

You can read more about `Regular Expression Denial of Service (ReDoS)` on our **blog <https://snyk.io/blog/redos-and-catastrophic-backtracking/>** .

Medium severity

Regular Expression Denial of Service (ReDoS)

Vulnerable module: **brace-expansion**

Introduced through: **knex-migrator@2.1.5** and **sqlite3@3.1.8**

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › knex-migrator@2.1.5 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › tar-pack@3.3.0 › fstream-ignore@1.0.5 › minimatch@3.0.3 › brace-expansion@1.1.6

  Remediation: Your dependencies are out of date, otherwise you would be using a newer brace-expansion than brace-expansion@1.1.6. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › tar-pack@3.3.0 › fstream-ignore@1.0.5 › minimatch@3.0.3 › brace-expansion@1.1.6

  Remediation: Your dependencies are out of date, otherwise you would be using a newer brace-expansion than brace-expansion@1.1.6. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › tar-pack@3.3.0 › rimraf@2.5.4 › glob@7.1.1 › minimatch@3.0.3 › brace-expansion@1.1.6

  Remediation: Your dependencies are out of date, otherwise you would be using a newer brace-expansion than brace-expansion@1.1.6. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

…and 11 more

Overview

`brace-expansion` **<https://www.npmjs.com/package/brace-expansion>** is a package that performs brace expansion as known from sh/bash. Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) attacks.

The Regular expression Denial of Service (ReDoS) is a type of Denial of Service attack. Many Regular Expression implementations may reach edge cases that causes them to work very slowly (exponentially related to input size), allowing an attacker to exploit this and can cause the program to enter these extreme situations by using a specially crafted input and cause the service to excessively consume CPU, resulting in a Denial of Service.

An attacker can provide a long value to the `expand` function, which nearly matches the pattern being matched. This will cause the regular expression matching to take a long time, all the while occupying the event loop and preventing it from processing other requests and making the server unavailable (a Denial of Service attack). Running:

```
const expand = require('brace-expansion');
            expand('{,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,\n}')
```

Will hang for long periods of time.

You can read more about `Regular Expression Denial of Service (ReDoS)` on our **blog** **<https://snyk.io/blog/redos-and-catastrophic-backtracking/>** .

Medium severity

Uninitialized Memory Exposure

Vulnerable module: **tunnel-agent**

Introduced through: **knex-migrator@2.1.5**, **sqlite3@3.1.8** and others

---

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › knex-migrator@2.1.5 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › request@2.76.0 › tunnel-agent@0.4.3

  Remediation: Your dependencies are out of date, otherwise you would be using a newer tunnel-agent than tunnel-agent@0.4.3. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › request@2.76.0 › tunnel-agent@0.4.3

  Remediation: Your dependencies are out of date, otherwise you would be using a newer tunnel-agent than tunnel-agent@0.4.3. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › knex-migrator@2.1.5 › ghost-ignition@2.8.14 › bunyan-loggly@1.1.0 › loggly@1.1.1 › request@2.75.0 › tunnel-agent@0.4.3

  Remediation: No remediation path available.

…and 3 more

Overview

`tunnel-agent` **<https://www.npmjs.com/package/tunnel-agent>** is HTTP proxy tunneling agent. Affected versions of the package are vulnerable to Uninitialized Memory Exposure.

A possible memory disclosure vulnerability exists when a value of type `number` is used to set the *proxy.auth* option of a request `request` and results in a possible uninitialized memory exposures in the request body.

This is a result of unobstructed use of the `Buffer` constructor, whose **insecure default constructor increases the odds of memory leakage <https://snyk.io/blog/exploiting-buffer/> .**

Medium severity

Uninitialized Memory Exposure

Vulnerable module: **concat-stream**

Introduced through: **gscan@1.1.7**, **multer@1.3.0** and others

---

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › gscan@1.1.7 › multer@1.1.0 › concat-stream@1.5.0

  Remediation: Your dependencies are out of date, otherwise you would be using a newer concat-stream than concat-stream@1.5.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › multer@1.3.0 › concat-stream@1.5.0

  Remediation: Your dependencies are out of date, otherwise you would be using a newer concat-stream than concat-stream@1.5.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › gscan@1.1.7 › extract-zip-fork@1.5.1 › concat-stream@1.5.0

  Remediation: No remediation path available.

…and 1 more

Overview

`concat-stream` **<https://www.npmjs.com/package/concat-stream>** is writable stream that concatenates strings or binary data and calls a callback with the result. Affected versions of the package are vulnerable to Uninitialized Memory Exposure.

A possible memory disclosure vulnerability exists when a value of type `number` is provided to the `stringConcat()` method and results in concatenation of uninitialized memory to the stream collection.

This is a result of unobstructed use of the `Buffer` constructor, whose **insecure default constructor increases the odds of memory leakage** **<https://snyk.io/blog/exploiting-buffer/>** .

Low severity

Denial of Service (DoS)

Vulnerable module: **superagent**

Introduced through: **superagent@3.5.2**

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › superagent@3.5.2

  Remediation: Upgrade to superagent@3.7.0.

Overview

`superagent` **<https://www.npmjs.com/package/superagent>** is elegant & feature rich browser / node HTTP with a fluent API.

Affected versions of the package are vulnerable to Denial of Service (DoS) attacks. It uncompresses responses in memory, and a server controlled by a malicious user may send a specially crafted zip file which will then unzip in the target server and will cause excessive CPU consumption. This is also known as a `Zip Bomb`.

Low severity

Regular Expression Denial of Service (ReDoS)

Vulnerable module: **ms**

Introduced through: **brute-knex@2.0.0**, **gscan@1.1.7** and others

---

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › brute-knex@2.0.0 › express@4.14.0 › serve-static@1.11.2 › send@0.14.2 › ms@0.7.2

  Remediation: Your dependencies are out of date, otherwise you would be using a newer ms than ms@0.7.2. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › gscan@1.1.7 › express@4.14.0 › serve-static@1.11.2 › send@0.14.2 › ms@0.7.2

  Remediation: Upgrade to gscan@1.2.1.

- *Introduced through*: ghost@1.6.2 › brute-knex@2.0.0 › express@4.14.0 › send@0.14.1 › ms@0.7.1

  Remediation: Your dependencies are out of date, otherwise you would be using a newer ms than ms@0.7.1. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

…and 12 more

Overview

`ms` **<https://www.npmjs.com/package/ms>** is a tiny millisecond conversion utility.

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) due to an incomplete fix for previously reported vulnerability **npm:ms:20151024 <https://snyk.io/vuln/npm:ms:20151024>** . The fix limited the length of accepted input string to 10,000 characters, and turned to be insufficient making it possible to block the

event loop for 0.3 seconds (on a typical laptop) with a specially crafted string passed to `ms()` function.

Proof of concept

```
ms = require('ms');
            ms('1'.repeat(9998) + 'Q') // Takes about ~0.3s
```

Note: Snyk's patch for this vulnerability limits input length to 100 characters. This new limit was deemed to be a breaking change by the author. Based on user feedback, we believe the risk of breakage is *very* low, while the value to your security is much greater, and therefore opted to still capture this change in a patch for earlier versions as well. Whenever patching security issues, we always suggest to run tests on your code to validate that nothing has been broken.

For more information on `Regular Expression Denial of Service (ReDoS)` attacks, go to our blog **<https://snyk.io/blog/redos-and-catastrophic-backtracking/>** .

Low severity

Regular Expression Denial of Service (ReDoS)

Vulnerable module: **mime**

Introduced through: **nodemailer@0.7.1**, **brute-knex@2.0.0** and others

---

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › nodemailer@0.7.1 › mailcomposer@0.2.12 › mime@1.2.11

  Remediation: Upgrade to nodemailer@1.0.0.

- *Introduced through*: ghost@1.6.2 › brute-knex@2.0.0 › express@4.14.0 › serve-static@1.11.2 › send@0.14.2 › mime@1.3.4

  Remediation: Your dependencies are out of date, otherwise you would be using a newer mime than mime@1.3.4. Try deleting node_modules, reinstalling and running

`snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › gscan@1.1.7 › express@4.14.0 › serve-static@1.11.2 › send@0.14.2 › mime@1.3.4
  Remediation: Upgrade to gscan@1.2.1.

…and 5 more

Overview

`mime` **<https://www.npmjs.com/package/mime>** is a comprehensive, compact MIME type module.

Affected versions of this package are vulnerable to Regular expression Denial of Service (ReDoS). It uses regex the following regex `/.*[\.\/\\]/` in its lookup, which can cause a slowdown of 2 seconds for 50k characters.

The Regular expression Denial of Service (ReDoS) is a type of Denial of Service attack. Many Regular Expression implementations may reach extreme situations that cause them to work very slowly (exponentially related to input size), allowing an attacker to exploit this and can cause the program to enter these extreme situations by using a specially crafted input and cause the service to excessively consume CPU, resulting in a Denial of Service.

You can read more about `Regular Expression Denial of Service (ReDoS)` on our **blog <https://snyk.io/blog/redos-and-catastrophic-backtracking/>** .

Low severity

Regular Expression Denial of Service (ReDoS)

Vulnerable module: **debug**

Introduced through: **brute-knex@2.0.0**, **knex-migrator@2.1.5** and others

---

Detailed paths and remediation

- *Introduced through*: ghost@1.6.2 › brute-knex@2.0.0 › knex@0.12.2 › debug@2.2.0

  Remediation: Upgrade to brute-knex@2.1.0.

- *Introduced through*: ghost@1.6.2 › knex-migrator@2.1.5 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › tar-pack@3.3.0 › debug@2.2.0

  Remediation: Your dependencies are out of date, otherwise you would be using a newer debug than debug@2.2.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

- *Introduced through*: ghost@1.6.2 › sqlite3@3.1.8 › node-pre-gyp@0.6.31 › tar-pack@3.3.0 › debug@2.2.0

  Remediation: Your dependencies are out of date, otherwise you would be using a newer debug than debug@2.2.0. Try deleting node_modules, reinstalling and running `snyk wizard`. If the problem persists, one of your dependencies may be bundling outdated modules.

…and 27 more

Overview

`debug` **<https://www.npmjs.com/package/debug>** is a JavaScript debugging utility modelled after Node.js core's debugging technique..

`debug` uses **printf-style <https://wikipedia.org/wiki/Printf_format_string>** formatting. Affected versions of this package are vulnerable to Regular expression Denial of Service (ReDoS) attacks via the the `%o` formatter (Pretty-print an Object all on a single line). It used a regular expression (`/\s*\n\s*/g`) in order to strip whitespaces and replace newlines with spaces, in order to join the data into a single line. This can cause a very low impact of about 2 seconds matching time for data 50k characters long.

The Regular expression Denial of Service (ReDoS) is a type of Denial of Service attack. Many Regular Expression implementations may reach extreme situations that cause them to work very slowly (exponentially related to input size), allowing an attacker to exploit this and can cause the program to enter these extreme situations by using a specially crafted input and cause the service to excessively consume CPU, resulting in a Denial of Service.

You can read more about `Regular Expression Denial of Service (ReDoS)` on our **blog <https://snyk.io/blog/redos-and-catastrophic-backtracking/>** .