

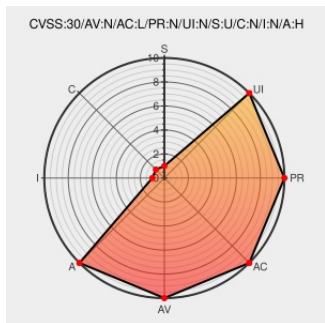


# CVE-2015-9242

Published on: 05/29/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

## CVE-2015-9242

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ecstatic](#) from [Ecstatic Project](#) contain the following vulnerability:

Certain input strings when passed to new Date() or Date.parse() in ecstatic node module before 1.4.0 will cause v8 to raise an exception. This leads to a crash and denial of service in ecstatic when this input is passed into the server via the If-Modified-Since header.

CVE-2015-9242 has been assigned by [h1](#) support@hackerone.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [h1](#) **HackerOne** - **ecstatic node module** version <1.4.0

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                                          | Tags                                                                                                 | Link                                                            |
|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Illegal access crash from if-modified-since header by substack · Pull Request #179 · jfhbrook/node-ecstatic · GitHub | <a href="#">Issue Tracking</a><br><a href="#">Third Party Advisory</a><br><a href="#">github.com</a> | <a href="#">MISC github.com/jfhbrook/node-ecstatic/pull/179</a> |

[github.com](#)  
[text/html](#)

Overview

[Third Party Advisory](#)  
[nodesecurity.io](#)  
[text/html](#)

 [MISC nodesecurity.io/advisories/64](#)

Issue 4640 - v8 - illegal access exception from Date strings - Monorail

[Issue Tracking](#)  
[Third Party Advisory](#)  
[bugs.chromium.org](#)  
[text/html](#)

 [MISC bugs.chromium.org/p/v8/issues/detail?id=4640](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

Related QID Numbers

[984057](#) Nodejs (npm) Security Update for ecstatic (GHSA-vwj-c-q9px-r9vq)

Known Affected Configurations (CPE V2.3)

| Type                                                               | Vendor                           | Product                  | Version | Update | Edition | Language |
|--------------------------------------------------------------------|----------------------------------|--------------------------|---------|--------|---------|----------|
| Application                                                        | <a href="#">Ecstatic Project</a> | <a href="#">Ecstatic</a> | All     | All    | All     | All      |
| Application                                                        | <a href="#">Ecstatic Project</a> | <a href="#">Ecstatic</a> | All     | All    | All     | All      |
| <div>cpe:2.3:a:ecstatic_project:ecstatic:*:*:*:*:node.js:*:*</div> |                                  |                          |         |        |         |          |
| <div>cpe:2.3:a:ecstatic_project:ecstatic:*:*:*:*:node.js:*:*</div> |                                  |                          |         |        |         |          |

No vendor comments have been submitted for this CVE