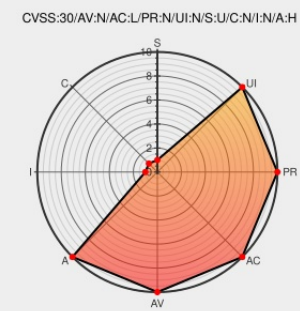
CVE-2015-9242

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 support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **HackerOne** - **ecstatic node module** version **<1.4.0**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Illegal access crash from if-modified-since header by substack · Pull Request #179 · jfhbrook/node-ecstatic · GitHub	Issue Tracking, Third Party Advisory, github.com	MISC github.com/jfhbrook/node-ecstatic/pull/179

	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

Related QID Numbers

984057 Nodejs (npm) Security Update for ecstatic (GHSA-vwjc-q9px-r9vq)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ecstatic Project	Ecstatic	All	All	All	All
Application	Ecstatic Project	Ecstatic	All	All	All	All

cpe:2.3:a:ecstatic_project:ecstatic:*:*:*:*:*:node.js:*:*:

cpe:2.3:a:ecstatic_project:ecstatic:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→