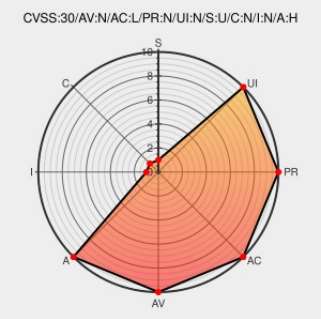
CVE-2017-16117

Published on: 06/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-16117

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Slug from Slug Project contain the following vulnerability:

slug is a module to slugify strings, even if they contain unicode. slug is vulnerable to regular expression denial of service is specially crafted untrusted input is passed as input. About 50k characters can block the event loop for 2 seconds.

CVE-2017-16117 has been assigned by support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **HackerOne** - **slug node module** version **All versions**

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
Overview	Third Party Advisory nodesecurity.io text/html	MISC nodesecurity.io/advisories/537

Vulnerable Regular Expression · Issue #82 · dodo/node-slug · GitHub	Third Party Advisory github.com text/html	MISC github.com/dodo/node-slug/issues/82

Related QID Numbers

983996 Nodejs (npm) Security Update for slug (GHSA-jxqq-cqm6-pfq9)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:slug_project:slug:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→