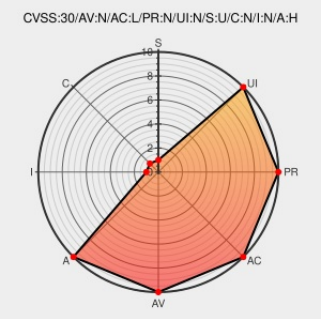
CVE-2018-11615

Published on: 08/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11615

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



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

This vulnerability allows remote attackers to deny service on vulnerable installations of npm mosca 2.8.1. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of topics. A crafted regular expression can cause the broker to crash. An attacker can leverage this vulnerability to deny access to the target system. Was ZDI-CAN-6306.

CVE-2018-11615 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **npm** - **npm mosca** version **2.8.1**

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: 7.8 - HIGH

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

CVE References

Description	Tags	Link

Description	Tags	Link
ZDI-18-583 | Zero Day Initiative	Third Party Advisory VDB Entry zerodayinitiative.com text/html	MISC zerodayinitiative.com/advisories/ZDI-18-583

Related QID Numbers

984068 Nodejs (npm) Security Update for mosca (GHSA-wqg7-vrj7-v82h)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mosca Project	Mosca	2.8.1	All	All	All
Application	Mosca Project	Mosca	2.8.1	All	All	All

cpe:2.3:a:mosca_project:mosca:2.8.1:*:*:*:*:node.js:*:*

cpe:2.3:a:mosca_project:mosca:2.8.1:*:*:*:*:node.js:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→