

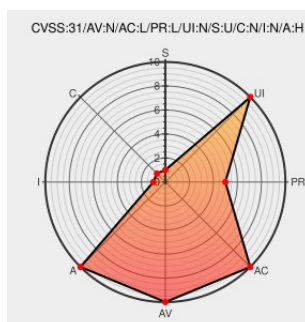


CVE-2018-20803

Published on: 11/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:35 PM UTC

CVE-2018-20803

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

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

A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which loop indefinitely in mathematics processing while retaining locks. This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.5; v3.6 versions prior to 3.6.10; v3.4 versions prior to 3.4.19.

CVE-2018-20803 has been assigned by cna@mongodb.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: MongoDB Inc. - MongoDB Server version < 4.0.5

Affected Vendor/Software: MongoDB Inc. - MongoDB Server version < 3.6.10

Affected Vendor/Software: MongoDB Inc. - MongoDB Server version < 3.4.19

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description

Tags

Link

[SERVER-38070] Infinite loop in aggregation expression - MongoDB

Issue Tracking

Patch

Vendor Advisory

jira.mongodb.org

text/html

MISC

jira.mongodb.org/browse/SERVER-38070

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mongodb	Mongodb	All	All	All	All
Application	Mongodb	Mongodb	All	All	All	All

cpe:2.3:a:mongodb:mongodb:*****:

cpe:2.3:a:mongodb:mongodb:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→