Group member: Samiya Kazi

Week 7

MongoDB Vulnerabilities Classified with Stanform Risk Classifications

CVE ID: CVE-2021-20333

Date published: 2021-07-23

Risk Classification: Low Data Risk

Description: Sending specially crafted commands to a MongoDB Server may result in artificial log entries being generated or for log entries to be split.

CVE ID: CVE-2021-20326

Date published: 2021-04-30

Risk Classification: Low Data Risk

Description: A user authorized to performing a specific type of find query may trigger a denial of service.

CVE ID: CVE-2020-7929

Date published: 2021-03-01

Risk Classification: Low Data Risk

Description: A user authorized to perform database queries may trigger denial of service by issuing specially crafted query contain a type of regex.

|  |
| --- |
|  |

CVE ID: CVE-2020-7928

Date published: 2020-11-23

Risk Classification: Moderate Data Risk

Description: A user authorized to perform database queries may trigger a read overrun and access arbitrary memory by issuing specially crafted queries.

CVE ID: CVE-2020-7926

Date published: 2020-11-23

Risk Classification: Low Data Risk

Description: A user authorized to perform database queries may cause denial of service by issuing a specially crafted query which violates an invariant in the server selection subsystem.

CVE ID: CVE-2020-7925

Date published: 2020-11-23

Risk Classification: Low Data Risk/Moderate Data Risk

Description: Incorrect validation of user input in the role name parser may lead to use of uninitialized memory allowing an unauthenticated attacker to use a specially crafted request to cause a denial of service.

CVE ID: CVE-2020-7923

Date published: 2020-08-21

Risk Classification: Low Data Risk

Description: A user authorized to perform database queries may cause denial of service by issuing specially crafted queries, which violate an invariant in the query subsystem's support for geoNear.

CVE ID: CVE-2020-7921

Date published: 2020-05-06

Risk Classification: High Data Risk

Description: Improper serialization of internal state in the authorization subsystem in MongoDB Server's authorization subsystem permits a user with valid credentials to bypass IP whitelisting protection mechanisms following administrative action.

CVE ID: CVE-2019-20925

Date published: 2020-11-24

Risk Classification: Moderate Data Risk

Description: An unauthenticated client can trigger denial of service by issuing specially crafted wire protocol messages, which cause the message decompressor to incorrectly allocate memory.

CVE ID: CVE-2019-20924

Date published: 2020-11-23

Risk Classification: Low Data Risk

Description: A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries which trigger an invariant in the IndexBoundsBuilder.

CVE ID: CVE-2019-20923

Date published: 2020-11-23

Risk Classification: Low Data Risk

Description: A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which throw unhandled Javascript exceptions containing types intended to be scoped to the Javascript engine's internals.

CVE ID: CVE-2019-2393

Date published: 2020-11-23

Risk Classification: Low Data Risk

Description: A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which use $lookup and collations.

CVE ID: CVE-2019-2392

Date published: 2020-11-23

Risk Classification: Low Data Risk

Description: A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which use the $mod operator to overflow negative values.

CVE ID: CVE-2019-2389

Date published: 2019-08-30

Risk Classification: Moderate Data Risk

Description: Incorrect scoping of kill operations in MongoDB Server's packaged SysV init scripts allow users with write access to the PID file to insert arbitrary PIDs to be killed when the root user stops the MongoDB process via SysV init.

CVE ID: CVE-2019-2386

Date published: 2019-08-06

Risk Classification: High Data Risk

Description: After user deletion in MongoDB Server the improper invalidation of authorization sessions allows an authenticated user's session to persist and become conflated with new accounts, if those accounts reuse the names of deleted ones.