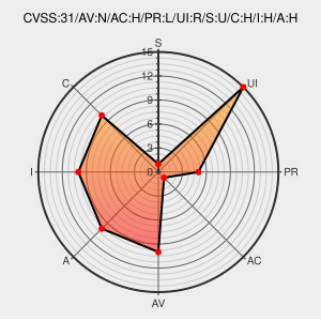
# CVE-2019-2386

Published on: 08/06/2019 12:00:00 AM UTC

Last Modified on: 06/19/2023 02:15:00 PM UTC

## CVE-2019-2386

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




Certain versions of Mongodb from Mongodb contain the following vulnerability:

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. This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.9; v3.6 versions prior to 3.6.13; v3.4 versions prior to 3.4.22.

CVE-2019-2386 has been assigned by cna@mongodb.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **MongoDB Inc.** - **MongoDB Server** version **< 4.0.9**

Affected Vendor/Software: **MongoDB Inc.** - **MongoDB Server** version **< 3.6.13**

Affected Vendor/Software: **MongoDB Inc.** - **MongoDB Server** version **< 3.4.22**

### Vulnerability Patch/Work Around

After deleting one or more users, restart any nodes which may have had active user authorization sessions.

Refrain from creating user accounts with the same name as previously deleted accounts.

### CVSS3 Score: 7.1 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | HIGH | LOW | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 6 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|

| Vector | Complexity | |
|---|---|---|
| NETWORK | MEDIUM | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

## CVE References

| Description | Tags | Link |
|---|---|---|
| TALOS-2019-0829 \|\| Cisco Talos Intelligence Group - Comprehensive Threat Intelligence | Exploit<br>Third Party Advisory<br>www.talosintelligence.com<br>text/html | MISC www.talosintelligence.com/vulnerability_reports/TALOS-2019-0829 |
| [SERVER-38984] Attach IDs to users - MongoDB | Vendor Advisory<br>jira.mongodb.org<br>text/html | CONFIRM jira.mongodb.org/browse/SERVER-38984 |



## Related QID Numbers

198471 Ubuntu Security Notification for MongoDB Vulnerability (USN-5052-1)

## 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→