



Memory safety issues in slot-based execution hash table spill

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2026-4358
State	PUBLISHED
Assigner	mongodb
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-17 20:16:15 UTC
Updated	2026-04-02 12:16:02 UTC
Description	A specially crafted aggregation query with \$lookup by an authenticated user with write privileges can cause a double-free o

Risk And Classification

Primary CVSS: v4.0 6.1 MEDIUM from cna@mongodb.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-415 | CWE-415 CWE-415 Double free

Version	Source	Type	Score	Severity	Vector
4.0	cna@mongodb.com	Secondary	6.1	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/E:X/
4.0	CNA	CVSS	6.1	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	cna@mongodb.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H
3.1	CNA	CVSS	6.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

CNA	MongoDB Inc	MongoDB Server	affected 8.2 8.2.6 custom	Not specified
CNA	MongoDB Inc	MongoDB Server	affected 8.0 8.0.20 custom	Not specified
CNA	MongoDB Inc	MongoDB Server	affected 7.0 7.0.31 custom	Not specified

References

Reference	Source	Link	Tags
jira.mongodb.org/browse/SERVER-118849	cna@mongodb.com	jira.mongodb.org	Exploit, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)