



Unbounded Memory Allocation in VQLResponse Result-Set Writer

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

Summary

CVE	CVE-2026-6948
State	PUBLISHED
Assigner	rapid7
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 00:16:39 UTC
Updated	2026-05-04 00:16:39 UTC
Description	Velociraptor versions prior to 0.76.4 contain a resource exhaustion vulnerability in the server's agent control channel. This a

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from cve@rapid7.com

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

Problem Types: CWE-770 | CWE-770 CWE-770 Allocation of resources without limits or throttling

Version	Source	Type	Score	Severity	Vector
3.1	cve@rapid7.com	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Rapid7	Velociraptor	affected 0.76.4 custom	Linux
CNA	Rapid7	Velociraptor	affected 0.75.9 custom	Linux

References

Reference	Source	Link	Tags
docs.velociraptor.app/announcements/advisories/cve-2026-6948	cve@rapid7.com	docs.velociraptor.app	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: We thank Faisal Alhumaid (Faisal.alhumaid@hotmail.com) for reporting this issue responsibly. (en)

CNA: We also thank Mika Jarvinen (mika.jarvinen@kapsi.fi) for reporting this issue responsibly at the same time. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-19T14:00:00.000Z	Initial report by Faisal Alhumaid
CNA	2026-04-19T14:00:00.000Z	Initial report by Mika Jarvinen
CNA	2026-04-27T23:50:00.000Z	Advisory published and patch distributed

Solutions

CNA: To remediate, you will need to upgrade your server <https://www.velociraptor-docs.org/docs/deployment/server/upgrades/#upgrading-a-server-in-place-upgrade> to the latest version of your release: * For 0.76 releases, upgrade immediately to v0.76.4 <https://github.com/Velocidex/velociraptor/releases/download/v0.76/velociraptor-v0.76.4-linux-amd64> * For 0.75 releases, upgrade immediately to v0.75.9 <https://github.com/Velocidex/velociraptor/releases/download/v0.75/velociraptor-v0.75.9-linux-amd64>

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](#).

Free CVE JSON API [cve.report/api](#)

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