



Rapid7 Velociraptor Improper Input Validation in Client Message Handler

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

Summary

CVE CVE-2026-5329

State PUBLISHED

Assigner rapid7

Source Priority CVE Program / NVD first with legacy fallback

Published 2026-04-09 18:17:04 UTC

Updated 2026-04-09 18:17:04 UTC

Description Rapid7 Velociraptor versions prior to 0.76.2 contain an improper input validation vulnerability in the client monitoring messa

Risk And Classification

Primary CVSS: v3.1 8.5 HIGH from cve@rapid7.com

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

Problem Types: CWE-20 | CWE-20 CWE-20 Improper input validation

Version	Source	Type	Score	Severity	Vector
3.1	cve@rapid7.com	Secondary	8.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	8.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Rapid7	Velociraptor	affected 0.76.1 semver	Linux
CNA	Rapid7	Velociraptor	affected 0.75.6 semver	Linux
CNA	Rapid7	Velociraptor	affected 0.74.6 semver	Linux

References

Reference	Source	Link	Tags
docs.velociraptor.app/announcements/advisories/cve-2026-5329	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 Chris Au (@netero_1010) from NyxLab for identifying and reporting this issue. (en)

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