



CVE-2023-46118

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-46118
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-25 18:17:00 UTC
Updated	2023-12-02 01:15:00 UTC
Description	RabbitMQ is a multi-protocol messaging and streaming broker. HTTP API did not enforce an HTTP request body limit, making it possible to cause a Denial of Service (DoS) by publishing large messages over the HTTP API.

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Rabbitmq	All	All	All	All

References

Reference	Source	Link
Denial of Service by publishing large messages over the HTTP API · Advisory · rabbitmq/rabbitmq-server · GitHub	MISC	github.com
www.debian.org/security/2023/dsa-5571		www.debian.org/security/2023/dsa-5571
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199939](#) Ubuntu Security Notification for RabbitMQ Vulnerability (USN-6501-1)

[242869](#) Red Hat Update for OpenStack Platform 17.1 (RHSA-2024:0217)

[6000369](#) Debian Security Update for rabbitmq-server (DSA 5571-1)

[6000382](#) Debian Security Update for rabbitmq-server (DLA 3687-1)

© [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](#)