



CVE-2014-9650

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

Summary

CVE	CVE-2014-9650
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-27 20:03:00 UTC
Updated	2023-11-07 02:23:00 UTC
Description	CRLF injection vulnerability in the management plugin in RabbitMQ 2.1.0 through 3.4.x before 3.4.1 allows remote attacker:

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pivotal Software	Rabbitmq	2.1.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.1.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.2.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.3.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.3.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.4.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.4.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.5.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.5.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.6.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.6.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.7.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.7.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.2	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.3	All	All	All

Application	Pivotal Software	Rabbitmq	2.8.4	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.5	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.6	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.7	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.0	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.1	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.2	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.3	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.4	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.0	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.1	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.2	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.3	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.4	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.5	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.0	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.1	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.2	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.3	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.4	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.0	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.1	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.2	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.3	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.4	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.5	All	All	All
Application	Pivotal Software	Rabbitmq	3.4.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.1.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.1.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.2.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.3.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.3.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.4.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.4.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.5.0	All	All	All

Application	Pivotal Software	Rabbitmq	2.5.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.6.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.6.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.7.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.7.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.0	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.1	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.2	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.3	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.4	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.5	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.6	All	All	All
Application	Pivotal Software	Rabbitmq	2.8.7	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.0	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.1	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.2	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.3	All	All	All
Application	Pivotal Software	Rabbitmq	3.0.4	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.0	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.1	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.2	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.3	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.4	All	All	All
Application	Pivotal Software	Rabbitmq	3.1.5	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.0	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.1	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.2	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.3	All	All	All
Application	Pivotal Software	Rabbitmq	3.2.4	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.0	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.1	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.2	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.3	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.4	All	All	All
Application	Pivotal Software	Rabbitmq	3.3.5	All	All	All

Application	Pivotal Software	Rabbitmq	3.4.0	All	All	All
Application	Vmware	Rabbitmq	2.1.0	All	All	All
Application	Vmware	Rabbitmq	2.1.1	All	All	All
Application	Vmware	Rabbitmq	2.2.0	All	All	All
Application	Vmware	Rabbitmq	2.3.0	All	All	All
Application	Vmware	Rabbitmq	2.3.1	All	All	All
Application	Vmware	Rabbitmq	2.4.0	All	All	All
Application	Vmware	Rabbitmq	2.4.1	All	All	All
Application	Vmware	Rabbitmq	2.5.0	All	All	All
Application	Vmware	Rabbitmq	2.5.1	All	All	All
Application	Vmware	Rabbitmq	2.6.0	All	All	All
Application	Vmware	Rabbitmq	2.6.1	All	All	All
Application	Vmware	Rabbitmq	2.7.0	All	All	All
Application	Vmware	Rabbitmq	2.7.1	All	All	All
Application	Vmware	Rabbitmq	2.8.0	All	All	All
Application	Vmware	Rabbitmq	2.8.1	All	All	All
Application	Vmware	Rabbitmq	2.8.2	All	All	All
Application	Vmware	Rabbitmq	2.8.3	All	All	All
Application	Vmware	Rabbitmq	2.8.4	All	All	All
Application	Vmware	Rabbitmq	2.8.5	All	All	All
Application	Vmware	Rabbitmq	2.8.6	All	All	All
Application	Vmware	Rabbitmq	2.8.7	All	All	All
Application	Vmware	Rabbitmq	3.0.0	All	All	All
Application	Vmware	Rabbitmq	3.0.1	All	All	All
Application	Vmware	Rabbitmq	3.0.2	All	All	All
Application	Vmware	Rabbitmq	3.0.3	All	All	All
Application	Vmware	Rabbitmq	3.0.4	All	All	All
Application	Vmware	Rabbitmq	3.1.0	All	All	All
Application	Vmware	Rabbitmq	3.1.1	All	All	All
Application	Vmware	Rabbitmq	3.1.2	All	All	All
Application	Vmware	Rabbitmq	3.1.3	All	All	All
Application	Vmware	Rabbitmq	3.1.4	All	All	All
Application	Vmware	Rabbitmq	3.1.5	All	All	All
Application	Vmware	Rabbitmq	3.2.0	All	All	All
Application	Vmware	Rabbitmq	3.2.1	All	All	All
Application	Vmware	Rabbitmq	3.2.2	All	All	All

Application	Vmware	Rabbitmq	3.2.3	All	All	All
Application	Vmware	Rabbitmq	3.2.4	All	All	All
Application	Vmware	Rabbitmq	3.3.0	All	All	All
Application	Vmware	Rabbitmq	3.3.1	All	All	All
Application	Vmware	Rabbitmq	3.3.2	All	All	All
Application	Vmware	Rabbitmq	3.3.3	All	All	All
Application	Vmware	Rabbitmq	3.3.4	All	All	All
Application	Vmware	Rabbitmq	3.3.5	All	All	All
Application	Vmware	Rabbitmq	3.4.0	All	All	All

References

Reference	Source	Link	Tags
Google Groups	CONFIRM	groups.google.com	
oss-security - CVE Request: XSS and response-splitting bugs in rabbitmq management plugin	MLIST	www.openwall.com	Mailing
RabbitMQ CVE-2014-9650 HTTP Response Splitting Vulnerability	BID	www.securityfocus.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
www.rabbitmq.com/release-notes/README-3.4.1.txt	CONFIRM	www.rabbitmq.com	Vendor
Google Groups		groups.google.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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