CVE-2022-31008

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-31008
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-06 18:16:00 UTC
Updated	2023-07-21 17:09:00 UTC
Description	RabbitMQ is a multi-protocol messaging and streaming broker. In affected versions the shovel and federation plugins perfo

Risk And Classification

Problem Types: CWE-335

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
Predictable credential obfuscation seed value used in Shovel and Federation plugins · Advisory · rabbitmq/rabbitmq-server · GitHub
Implement fallback secret for credentials obfuscation (by @luos) by michaelklishin · Pull Request #4841 · rabbitmq/rabbitmq-server · GitHub
cve-website
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

182193 Debian Security Update for rabbitmq-server (CVE-2022-31008)

752987 SUSE Enterprise Linux Security Update for rabbitmq-server (SUSE-SU-2022:4378-1)

© 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 registred 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