



CVE-2020-25640

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

Summary

CVE	CVE-2020-25640
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-24 19:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	A flaw was discovered in WildFly before 21.0.0.Final where, Resource adapter logs plain text JMS password at warning lev

Risk And Classification

Problem Types: CWE-532

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Wildfly	All	All	All	All
Application	Redhat	Wildfly	All	All	All	All

References

Reference

- 1881637 – (CVE-2020-25640) CVE-2020-25640 wildfly: resource adapter logs plaintext JMS password at warning level on connection error
- JMS Connection password logged in cleartext · Issue #13 · amqphub/amqp-10-resource-adapter · GitHub
- CVE-2020-25640 WildFly Vulnerability in NetApp Products | NetApp Product Security
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](#).

CVE.report and Source URL Uptime Status status.cve.report