



CVE-2022-0866

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

Summary

CVE	CVE-2022-0866
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-10 21:15:00 UTC
Updated	2022-05-18 16:13:00 UTC
Description	This is a concurrency issue that can result in the wrong caller principal being returned from the session context of an EJB th

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Enterprise Application Platform	All	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All
Application	Redhat	Wildfly	All	All	All	All

References

Reference

- [2060929 – \(CVE-2022-0866\) CVE-2022-0866 wildfly: Wildfly management of EJB Session context returns wrong caller principal with Elytron S](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [240458](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.5 on RHEL 7 (RHSA-2022:4918)
- [240459](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.5 on RHEL 8 (RHSA-2022:4919)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)