



CVE-2014-8122

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

Summary

CVE	CVE-2014-8122
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-13 15:59:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	Race condition in JBoss Weld before 2.2.8 and 3.x before 3.0.0 Alpha3 allows remote attackers to obtain information from s

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Weld	3.0.0	alpha1	All	All
Application	Redhat	Jboss Weld	3.0.0	alpha2	All	All
Application	Redhat	Jboss Weld	3.0.0	alpha1	All	All
Application	Redhat	Jboss Weld	3.0.0	alpha2	All	All
Application	Redhat	Jboss Weld	All	All	All	All

References

Reference
WELD-1802 An exception during context deactivation/dissociation should · weld/core@8e41320 · GitHub
WELD-1802 RequestScopedCache - Make sure each request is ended before... · weld/core@6808b11 · GitHub
Red Hat JBoss Weld CVE-2014-8122 Information Disclosure Vulnerability
Red Hat Customer Portal
victims-cve-db/8122.yaml at master · victims/victims-cve-db · GitHub
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal

Red Hat JBoss Enterprise Application Platform Bugs Let Remote Users Obtain Potentially Sensitive Information and Remote Authenticated Users
WELD-1802 RequestScopedCache - Testcase · weld/core@29fd110 · GitHub
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
RHSA-2015:0920
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
Legacy QID Mappings
981450 Java (maven) Security Update for org.jboss.weld:weld-core-bom (GHSA-338v-3958-8v8r)