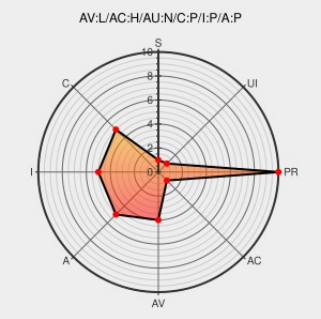
CVE-2012-4572

Published on: 10/28/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:13 AM UTC

CVE-2012-4572

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Jboss Enterprise Application Platform from Redhat contain the following vulnerability:

Red Hat JBoss Enterprise Application Platform (EAP) before 6.1.0 and JBoss Portal before 6.1.0 does not load the implementation of a custom authorization module for a new application when an implementation is already loaded and the modules share class names, which allows local users to control certain applications' authorization decisions via a crafted application.

CVE-2012-4572 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 3.7 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Red Hat Customer Portal	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:0834
Red Hat Customer Portal	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:0833
Red Hat Customer Portal	Vendor Advisory, web.archive.org, text/html	REDHAT RHSA-2013:1437

Inactive Link | Not Archived

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.0.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.2	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.2.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.2.2	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.0.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.2	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.2.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.2.2	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	All	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.0.1	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.1.0	All	All	All

Application	Redhat	Jboss Enterprise Portal Platform	5.1.1	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.2.0	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.2.1	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.2.2	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.0.1	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.1.1	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.2.0	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.2.1	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	5.2.2	All	All	All
Application	Redhat	Jboss Enterprise Portal Platform	All	All	All	All

cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.2.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.0.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.1.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.1.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.1.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.2.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.2.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.2.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.2.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.0.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.1.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.1.1:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.1.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_application_platform:6.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_application_platform:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:4.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:4.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:jboss_enterprise_portal_platform:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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