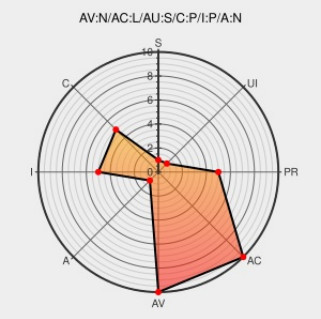
CVE-2013-2133

Published on: 12/06/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:25 AM UTC

CVE-2013-2133

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



Certain versions of Enterprise Linux from Redhat contain the following vulnerability:

The EJB invocation handler implementation in Red Hat JBossWS, as used in JBoss Enterprise Application Platform (EAP) before 6.2.0, does not properly enforce the method level restrictions for JAX-WS Service endpoints, which allows remote authenticated users to access otherwise restricted JAX-WS handlers by leveraging permissions to the EJB class.

CVE-2013-2133 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:1785
Red Hat Customer Portal	web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2015:0850
Red Hat Customer Portal	web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2015:0851

Red Hat Customer Portal	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1786
JBoss Enterprise Application Platform Bugs Let Local Users Gain Elevated Privileges and Remote Authenticated Users Bypass Security Controls - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1029431
Red Hat Customer Portal	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1784

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp09	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp10	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	6.0.1	All	All	All

Application	Redhat	Jboss Enterprise Application Platform	4.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.2.0	cp09	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	4.3.0	cp10	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	6.0.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	All	All	All	All

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

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

cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.2.0:cp09:*:*:*:*:*:*:

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

cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp10:*:*:*:*:*:*:

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:6.0.1:*:*:*:*:*:*:*

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

cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.2.0:cp09:*:*:*:*:*:

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

cpe:2.3:a:redhat:jboss_enterprise_application_platform:4.3.0:cp10:*:*:*:*:*:

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:6.0.1:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→