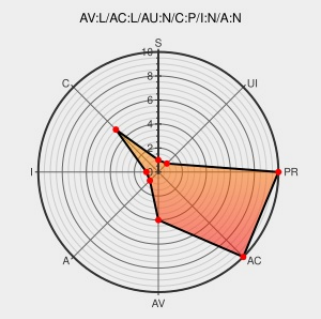
CVE-2000-1247

Published on: 10/04/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:29 PM UTC

CVE-2000-1247

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



Certain versions of Jserv from Apache contain the following vulnerability:

The default configuration of the jserv-status handler in jserv.conf in Apache JServ 1.1.2 includes an "allow from 127.0.0.1" line, which allows local users to discover JDBC passwords or other sensitive information via a direct request to the jserv/ URI.

CVE-2000-1247 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
jserv wrapper error - CXSecurity.com	securityreason.com, text/html	SREASON 8412
	Patch, archive.apache.org, application/gzip	CONFIRM archive.apache.org/dist/java/java.apache.org-www.tar.gz
'jserv wrapper error' - MARC	Exploit, marc.info, text/html	MLIST [java-apache-users] 20000929 jserv wrapper error
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF apache-jserv-env-information-disclosure(51946)

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	Apache	Jserv	1.1.2	All	All	All
Application	Apache	Jserv	1.1.2	All	All	All

cpe:2.3:a:apache:jserv:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:apache:jserv:1.1.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→