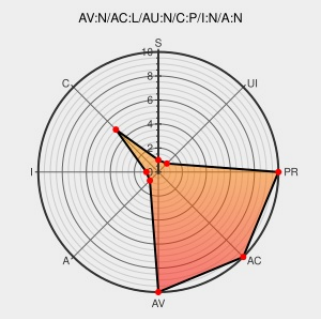
# CVE-2005-4834

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

## CVE-2005-4834

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




Certain versions of Websphere Application Server from Ibm contain the following vulnerability:

IBM WebSphere Application Server (WAS) 5.0.2.5 through 5.1.1.3 allows remote attackers to obtain JSP source code and other sensitive information, related to incorrect request processing by the web container.

CVE-2005-4834 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 5 - MEDIUM

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

### CVE References

| Description | Tags | Link |
|---|---|---|
| WebSphere Application Server JSP Source Code Disclosure - Advisories - Secunia | Vendor Advisory, web.archive.org, text/html | SECUNIA 24478 |
| IBM WebSphere Application Server Source Code Disclosure Vulnerability | cve.report (archive), text/html | BID 22991 |
| IBM notice: The page you requested cannot be displayed | Patch, Vendor Advisory, www-1.ibm.com, text/html, Inactive Link, Not Archived | AIXAPAR PQ99537 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | www.vupen.com, text/html | VUPEN ADV-2007-0970 |
| IBM Possible security exposure with JavaServer Page (JSP) and IBM | Patch | CONFIRM www- |

| | | |
|---|---|---|
| WebSphere Application Server (PK23475, PK32374, PK22928, PK00091, PQ91033, PQ99537, PK28963, PK20181, PK23670) - United States | Vendor Advisory<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | 1.ibm.com/support/docview.wss?uid=swg21243541 |
| IBM notice: The page you requested cannot be displayed | Patch<br>Vendor Advisory<br>www-1.ibm.com<br>text/html<br>Inactive Link Not Archived | AIXAPAR PK28963 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Ibm | Websphere Application Server | 5.0.2.5 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.0.2.6 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.0.2.7 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.0.2.8 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.0.2.9 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.0 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.0.2 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.0.3 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.0.4 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.0.5 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.1 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.1.2 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.1.3 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.0.2.5 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.0.2.6 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.0.2.7 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.0.2.8 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.0.2.9 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.0 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.0.2 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.0.3 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.0.4 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Ibm | Websphere Application Server | 5.1.0.5 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.1 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.1.2 | All | All | All |
| Application | Ibm | Websphere Application Server | 5.1.1.3 | All | All | All |

cpe:2.3:a:ibm:websphere_application_server:5.0.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.0.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.0.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.0.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.0.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.0.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.0.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.0.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.0.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.0.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:5.1.1.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→