

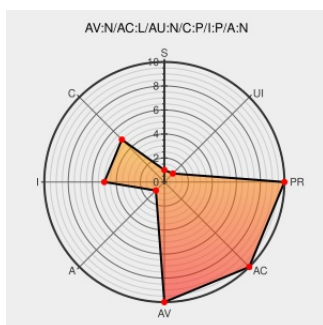


CVE-2006-1093

Published on: 03/09/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1093

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Websphere Application Server](#) from [Ibm](#) contain the following vulnerability:

Unspecified vulnerability in IBM WebSphere 5.0.2.10 through 5.0.2.15 and 5.1.1.4 through 5.1.1.9 allows remote attackers to obtain sensitive information via unknown attack vectors, which causes JSP source code to be revealed.

CVE-2006-1093 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2006-0788](#)

IBM notice: The page you requested cannot be displayed

[www-1.ibm.com](#)
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM www-1.ibm.com/support/docview.wss?uid=swg21231377](#)

IBM WebSphere Application Server JSP Source Code Disclosure Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[BID 16908](#)

SecurityTracker.com Archives - IBM WebSphere Application Server May Disclose JavaServer Pages Source to Remote Users

[Vendor Advisory](#)
[securitytracker.com](#)
[text/html](#)

[SECTrack 1015716](#)

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,

are more appropriate for your purposes. CVEreport does not necessarily endorse the views expressed, or content, that are linked presented on these sites. 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	Ibm	Websphere Application Server	5.0.2	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.1	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.10	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.11	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.12	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.13	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.14	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.2	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.3	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.4	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	5.1.1	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.1	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	5.1.1.4	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.5	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.6	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.7	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.8	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.9	All	All	All
Application	Ibm	Websphere Application Server	5.0.2	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.1	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.10	All	All	All
Application	Ibm	Websphere Application Server	5.0.2.11	All	All	All

Application	lbn	Websphere Application Server	5.0.2.12	All	All	All
Application	lbn	Websphere Application Server	5.0.2.13	All	All	All
Application	lbn	Websphere Application Server	5.0.2.14	All	All	All
Application	lbn	Websphere Application Server	5.0.2.2	All	All	All
Application	lbn	Websphere Application Server	5.0.2.3	All	All	All
Application	lbn	Websphere Application Server	5.0.2.4	All	All	All
Application	lbn	Websphere Application Server	5.0.2.5	All	All	All
Application	lbn	Websphere Application Server	5.0.2.6	All	All	All
Application	lbn	Websphere Application Server	5.0.2.7	All	All	All
Application	lbn	Websphere Application Server	5.0.2.8	All	All	All
Application	lbn	Websphere Application Server	5.0.2.9	All	All	All
Application	lbn	Websphere Application Server	5.1.1	All	All	All
Application	lbn	Websphere Application Server	5.1.1.1	All	All	All
Application	lbn	Websphere Application Server	5.1.1.2	All	All	All
Application	lbn	Websphere Application Server	5.1.1.3	All	All	All
Application	lbn	Websphere Application Server	5.1.1.4	All	All	All
Application	lbn	Websphere Application Server	5.1.1.5	All	All	All
Application	lbn	Websphere Application Server	5.1.1.6	All	All	All
Application	lbn	Websphere Application Server	5.1.1.7	All	All	All
Application	lbn	Websphere Application Server	5.1.1.8	All	All	All
Application	lbn	Websphere Application Server	5.1.1.9	All	All	All
cpe:2.3:a:ibm:websphere_application_server:5.0.2:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:5.0.2.1:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:5.0.2.10:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:5.0.2.11:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:5.0.2.12:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:5.0.2.13:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:5.0.2.14:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:5.0.2.2:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:5.0.2.3:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:5.0.2.4:*:*:*:*:*:						
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:5.1.1:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.1.1.1:*:*:*:*:*.*
```

```
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:5.1.1.4:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.1.1.5:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.1.1.6:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.1.1.7:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.1.1.8:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:5.1.1.9:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2:*.:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2.1:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2.10:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2.11:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2.12:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2.13:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2.14:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2.2:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2.3:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:5.0.2.4:*.~*~*~*~*~*~*
```

```
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:5.1.1:*:*:*:*:*:
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:5.1.1.4.*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:5.1.1.5.*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:5.1.1.6.*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:5.1.1.7.*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:5.1.1.8.*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:5.1.1.9.*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)