



# CVE-2006-3231

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2006-3231   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2006-06-27 10:05:00 UTC   |
| <b>Updated</b>         | 2019-10-09 22:50:00 UTC   |
| <b>Description</b>     | Unspecified vulnerability in IBM WebSphere Application Server (WAS) before 6.0.2.11, when fileServingEnabled is true, all |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product                      | Version | Update | Edition | Language |
|-------------|--------|------------------------------|---------|--------|---------|----------|
| Application | ibm    | WebSphere Application Server | 2.0     | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.0     | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.0.2   | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.0.2.1 | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.0.2.2 | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.0.2.3 | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.0.2.4 | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.5     | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.5.1   | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.5.2   | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 3.5.3   | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 4.0.3   | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 4.0.4   | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 5.0     | All    | All     | All      |
| Application | ibm    | WebSphere Application Server | 5.0.1   | 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 | 5.1.1.1  | All | All | All |
| Application | ibm | Websphere Application Server | 5.1.1.10 | 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 | 6.0      | All | All | All |
| Application | ibm | Websphere Application Server | 6.0.2    | All | All | All |
| Application | ibm | Websphere Application Server | 6.0.2.9  | All | All | All |

## References

### Reference

[IBM WebSphere Application Server Multiple Vulnerabilities - Advisories - Secunia](#)

[WebSphere Application Server JSP Source Code Disclosure - Advisories - Secunia](#)

[IBM WebSphere Application Server Source Code Disclosure Vulnerability](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[IBM Fix list for WebSphere Application Server Version 6.0.2 - United States](#)

[IBM Possible security exposure with JavaServer Page \(JSP\) and IBM WebSphere Application Server \(PK23475, PK32374, PK22928, PK0009\)](#)

[IBM Websphere Application Server Prior to 6.0.2.11 Multiple Vulnerabilities](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web](#)

[site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)