



CVE-2006-0431

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2006-0431
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-01-25 23:07:00 UTC
Updated	2017-07-20 01:29:00 UTC
Description	Unspecified vulnerability in BEA WebLogic Server and WebLogic Express 8.1 SP5 allows untrusted applications to obtain th

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bea	Weblogic Server	8.1	sp5	All	All
Application	Bea	Weblogic Server	8.1	sp5	express	All
Application	Bea	Weblogic Server	8.1	sp5	All	All
Application	Bea	Weblogic Server	8.1	sp5	express	All

References

Reference
BEA WebLogic Server/Express Vulnerabilities and Security Issues - Advisories - Secunia
BEA WebLogic Multiple Vulnerabilities
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
IBM X-Force Exchange
Server's SSL identity not properly protected from applications.
SecurityTracker.com Archives - BEA WebLogic Multiple Bugs Let Remote Users Deny Service, Obtain Information, and Access Restricted Re
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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)