



CVE-2007-0415

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

Summary

CVE	CVE-2007-0415
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-23 00:28:00 UTC
Updated	2011-03-08 02:49:00 UTC
Description	BEA WebLogic Server 8.1 through 8.1 SP5 does not properly enforce access control after a dynamic update and dynamic r

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	All	All	All
Application	Bea	Weblogic Server	8.1	All	All	All
Application	Bea	Weblogic Server	All	sp5	All	All

References

Reference	Source	Link
BEA Multiple Products Multiple Vulnerabilities	BID	www
BEA WebLogic Multiple Vulnerabilities and Security Issues - Advisories - Secunia	SECUNIA	secu
Dynamic updates to applications deployed as exploded jars may result in incorrect access checking	BEA	dev2
38509	OSVDB	osvd
Webmail - OVH	VUPEN	www
SecurityTracker.com Archives - WebLogic Bugs Let Remote Users Gain Access, Obtain Information, and Deny Service	SECTRACK	secu
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

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](#)