



# CVE-2008-0901

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

## Summary

<b>CVE</b>	CVE-2008-0901
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-02-22 21:44:00 UTC
<b>Updated</b>	2018-10-15 22:03:00 UTC
<b>Description</b>	BEA WebLogic Server and Express 7.0 through 10.0 allows remote attackers to conduct brute force password guessing att

## Risk And Classification

**Problem Types:** CWE-255 | CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bea	Weblogic Server	10.0	All	All	All
Application	Bea	Weblogic Server	7.0	All	All	All
Application	Bea	Weblogic Server	7.0	sp1	All	All
Application	Bea	Weblogic Server	7.0	sp2	All	All
Application	Bea	Weblogic Server	7.0	sp3	All	All
Application	Bea	Weblogic Server	7.0	sp4	All	All
Application	Bea	Weblogic Server	7.0	sp5	All	All
Application	Bea	Weblogic Server	7.0	sp6	All	All
Application	Bea	Weblogic Server	7.0	sp7	All	All
Application	Bea	Weblogic Server	8.1	All	All	All
Application	Bea	Weblogic Server	8.1	sp1	All	All
Application	Bea	Weblogic Server	8.1	sp2	All	All
Application	Bea	Weblogic Server	8.1	sp3	All	All
Application	Bea	Weblogic Server	8.1	sp4	All	All
Application	Bea	Weblogic Server	8.1	sp5	All	All
Application	Bea	Weblogic Server	8.1	sp6	All	All
Application	Bea	Weblogic Server	9.0	All	All	All

Application	Bea	Weblogic Server	9.1	All	All	All
Application	Bea	Weblogic Server	9.2	All	All	All
Application	Bea	Weblogic Server	9.2	mp1	All	All
Application	Bea	Weblogic Server	9.2	mp2	All	All
Application	Bea	Weblogic Server	10.0	All	All	All
Application	Bea	Weblogic Server	7.0	All	All	All
Application	Bea	Weblogic Server	7.0	sp1	All	All
Application	Bea	Weblogic Server	7.0	sp2	All	All
Application	Bea	Weblogic Server	7.0	sp3	All	All
Application	Bea	Weblogic Server	7.0	sp4	All	All
Application	Bea	Weblogic Server	7.0	sp5	All	All
Application	Bea	Weblogic Server	7.0	sp6	All	All
Application	Bea	Weblogic Server	7.0	sp7	All	All
Application	Bea	Weblogic Server	8.1	All	All	All
Application	Bea	Weblogic Server	8.1	sp1	All	All
Application	Bea	Weblogic Server	8.1	sp2	All	All
Application	Bea	Weblogic Server	8.1	sp3	All	All
Application	Bea	Weblogic Server	8.1	sp4	All	All
Application	Bea	Weblogic Server	8.1	sp5	All	All
Application	Bea	Weblogic Server	8.1	sp6	All	All
Application	Bea	Weblogic Server	9.0	All	All	All
Application	Bea	Weblogic Server	9.1	All	All	All
Application	Bea	Weblogic Server	9.2	All	All	All
Application	Bea	Weblogic Server	9.2	mp1	All	All
Application	Bea	Weblogic Server	9.2	mp2	All	All
Application	Bea Systems	Weblogic Server	10.0_mp1	All	All	All
Application	Bea Systems	Weblogic Server	10.0_mp1	All	All	All

## References

Reference	Source	Link	Tags
Page not found – S21Sec	MISC	<a href="http://www.s21sec.com">www.s21sec.com</a>	
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
Oracle Fusion Middleware Technologies	BEA	<a href="http://dev2dev.bea.com">dev2dev.bea.com</a>	Patch
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>	
WebLogic Lets Remote Users Bypass the Account Lockout Feature - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>	

About Secunia Research   Flexera	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical,

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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