

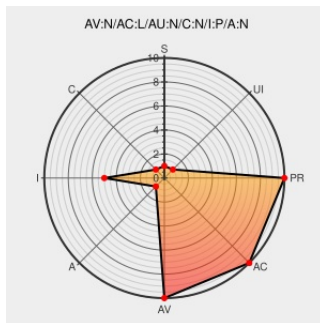


CVE-2004-1756

Published on: 04/13/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1756

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

Certain versions of [Weblogic Server](#) from [Bea](#) contain the following vulnerability:

BEA WebLogic Server and WebLogic Express 8.1 SP2 and earlier, and 7.0 SP4 and earlier, when using 2-way SSL with a custom trust manager, may accept a certificate chain even if the trust manager rejects it, which allows remote attackers to spoof other users or servers.

CVE-2004-1756 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
US-CERT Vulnerability Note VU#566390	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#566390
Advisories & Notifications	Patch Vendor Advisory dev2dev.bea.com text/html	CONFIRM dev2dev.bea.com/resource/library/advisoriesnotifications/BEA04_54.00.jsp
Secunia - Advisories - BEA WebLogic SSL Impersonation Vulnerability	Patch Vendor Advisory web.archive.org text/html	SECUNIA 11358

BEA WebLogic Server and WebLogic Express Certificate Chain User Impersonation Vulnerability

Patch

Vendor Advisory

cve.report (archive)

text/html

 BID 10132

IBM X-Force Exchange

exchange.xforce.ibmcloud.com

text/html

 XF weblogic-trust-certificate-spoofing(15862)

BEA WebLogic Custom Trust Manager Flaw May Let Remote Users Impersonate Target Users or Servers - SecurityTracker

Patch

Vendor Advisory

securitytracker.com

text/html

 SECTRACK 1009765

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, 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	Bea	Weblogic Server	7.0	All	express	All
Application	Bea	Weblogic Server	7.0	All	win32	All
Application	Bea	Weblogic Server	7.0	sp1	All	All
Application	Bea	Weblogic Server	7.0	sp1	express	All
Application	Bea	Weblogic Server	7.0	sp2	All	All
Application	Bea	Weblogic Server	7.0	sp2	express	All
Application	Bea	Weblogic Server	7.0	sp3	All	All
Application	Bea	Weblogic Server	7.0	sp3	express	All
Application	Bea	Weblogic Server	7.0	sp4	All	All
Application	Bea	Weblogic Server	7.0	sp4	express	All
Application	Bea	Weblogic Server	7.0	sp4	win32	All
Application	Bea	Weblogic Server	8.1	All	All	All
Application	Bea	Weblogic Server	8.1	All	express	All
Application	Bea	Weblogic Server	8.1	All	win32	All
Application	Bea	Weblogic Server	8.1	sp1	All	All
Application	Bea	Weblogic Server	8.1	sp1	express	All
Application	Bea	Weblogic Server	8.1	sp1	win32	All
Application	Bea	Weblogic Server	8.1	sp2	All	All
Application	Bea	Weblogic Server	8.1	sp2	express	All
Application	Bea	Weblogic Server	8.1	sp2	win32	All

cpe:2.3:a:bea:weblogic_server:8.1.*:express:****.*:
cpe:2.3:a:bea:weblogic_server:8.1.*:win32:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp1:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp1:express:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp1:win32:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp2:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp2:express:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp2:win32:****.*:
cpe:2.3:a:bea:weblogic_server:7.0.*:express:****.*:
cpe:2.3:a:bea:weblogic_server:7.0.*:win32:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp1:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp1:express:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp2:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp2:express:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp3:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp3:express:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp4:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp4:express:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp4:win32:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:****.*:
cpe:2.3:a:bea:weblogic_server:8.1.*:express:****.*:
cpe:2.3:a:bea:weblogic_server:8.1.*:win32:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp1:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp1:express:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp1:win32:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp2:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp2:express:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp2:win32:****.*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2023   |

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](#).

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