

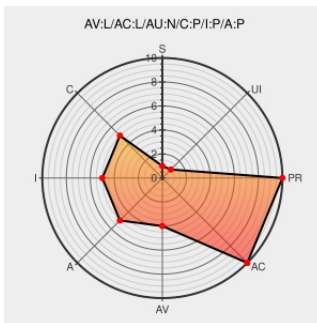


CVE-2005-4752

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4752

[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 SP4 and earlier, and 7.0 SP6 and earlier, might allow local users to gain privileges by using the run-as deployment descriptor element to change the privileges of a web application or EJB from the Deployer security role to the Admin security role.

CVE-2005-4752 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

BEA WebLogic Server and WebLogic Express Multiple Vulnerabilities

[Third Party Advisory](#)
[Vendor Advisory](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐 BID 15052](#)

A Deployed application can change privileges from Deployer to Admin.

[Patch](#)
[Vendor Advisory](#)
[dev2dev.bea.com](#)
[text/html](#)

[🔗 BEA BEA05-88.00](#)

Secunia - Advisories - BEA WebLogic 24 Vulnerabilities and Security Issues

[Third Party Advisory](#)
[web.archive.org](#)
[text/html](#)

[X SECUNIA 17138](#)

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	All	All
Application	Bea	Weblogic Server	7.0	All	express	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	sp5	All	All
Application	Bea	Weblogic Server	7.0	sp5	express	All
Application	Bea	Weblogic Server	7.0	sp6	All	All
Application	Bea	Weblogic Server	7.0	sp6	express	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	sp1	All	All
Application	Bea	Weblogic Server	8.1	sp1	express	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	sp3	All	All
Application	Bea	Weblogic Server	8.1	sp3	express	All
Application	Bea	Weblogic Server	8.1	sp4	All	All
Application	Bea	Weblogic Server	8.1	sp4	express	All
Application	Bea	Weblogic Server	7.0	All	All	All
Application	Bea	Weblogic Server	7.0	All	express	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	sp5	All	All
Application	Bea	Weblogic Server	7.0	sp5	express	All
Application	Bea	Weblogic Server	7.0	sp6	All	All
Application	Bea	Weblogic Server	7.0	sp6	express	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	sp1	All	All
Application	Bea	Weblogic Server	8.1	sp1	express	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	sp3	All	All
Application	Bea	Weblogic Server	8.1	sp3	express	All
Application	Bea	Weblogic Server	8.1	sp4	All	All
Application	Bea	Weblogic Server	8.1	sp4	express	All
cpe:2.3:a:bea:weblogic_server:7.0:*:*:*:*:*:						
cpe:2.3:a:bea:weblogic_server:7.0*:express:*:*:*:*:						
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:sp5:*:*:*:*:*:						
cpe:2.3:a:bea:weblogic_server:7.0:sp5:express:*:*:*:*:						
cpe:2.3:a:bea:weblogic_server:7.0:sp6:*:*:*:*:*:						

cpe:2.3:a:bea:weblogic_server:7.0:sp6:express:****.*:
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:sp1:****.*.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp1:express:****.*:
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:sp3:****.*.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp3:express:****.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp4:****.*.*:
cpe:2.3:a:bea:weblogic_server:8.1:sp4:express:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:****.*.*.*:
cpe:2.3:a:bea:weblogic_server:7.0:*:express:****.*:
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:sp5:****.*.*.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp5:express:****.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp6:****.*.*.*:
cpe:2.3:a:bea:weblogic_server:7.0:sp6:express:****.*:
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:sp1:****.*.*.*:

cpe:2.3:a:bea:weblogic_server:8.1:sp1:express:*****:
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:sp3:*****:
cpe:2.3:a:bea:weblogic_server:8.1:sp3:express:*****:
cpe:2.3:a:bea:weblogic_server:8.1:sp4:*****:
cpe:2.3:a:bea:weblogic_server:8.1:sp4:express:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)