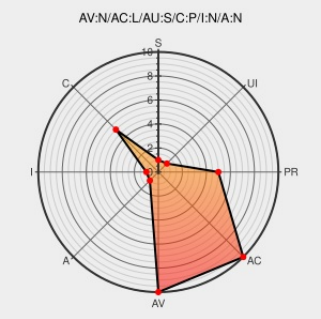
CVE-2006-2467

Published on: 05/19/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:09 PM UTC

CVE-2006-2467

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Weblogic Server from Bea contain the following vulnerability:

BEA WebLogic Server 8.1 up to SP4, 7.0 up to SP6, and 6.1 up to SP7 displays the internal IP address of the WebLogic server in the WebLogic Server Administration Console, which allows remote authenticated administrators to determine the address.

CVE-2006-2467 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2006-1828
WebLogic Server Console Displays the Domain Name Prior to Authentication - SecurityTracker	securitytracker.com, text/html	SECTRACK 1016099
WebLogic Server May Incorrectly Remove JDBC Security Policies - SecurityTracker	securitytracker.com, text/html	SECTRACK 1016097
BEA WebLogic Server/Express Multiple Security Issues - Advisories - Secunia	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 20130
Console displays the WebLogic Server IP address	Patch, Vendor Advisory, dev2dev.bea.com	BEA BEA06-129.00

	text/html	
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF weblogic-console-ip-disclosure(26462)

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	6.1	All	All	All
Application	Bea	Weblogic Server	6.1	sp1	All	All
Application	Bea	Weblogic Server	6.1	sp2	All	All
Application	Bea	Weblogic Server	6.1	sp3	All	All
Application	Bea	Weblogic Server	6.1	sp4	All	All
Application	Bea	Weblogic Server	6.1	sp5	All	All
Application	Bea	Weblogic Server	6.1	sp6	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	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	6.1	All	All	All
Application	Bea	Weblogic Server	6.1	sp1	All	All
Application	Bea	Weblogic Server	6.1	sp2	All	All
Application	Bea	Weblogic Server	6.1	sp3	All	All
Application	Bea	Weblogic Server	6.1	sp4	All	All
Application	Bea	Weblogic Server	6.1	sp5	All	All
Application	Bea	Weblogic Server	6.1	sp6	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	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

cpe:2.3:a:bea:weblogic_server:6.1:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp3:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp4:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp5:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp6:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp5:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:8.1:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:8.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:8.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:8.1:sp3:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp3:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp4:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp5:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:6.1:sp6:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:7.0:sp5:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:8.1:*:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:8.1:sp1:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:8.1:sp2:*:*:*:*:*:*:

cpe:2.3:a:bea:weblogic_server:8.1:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→