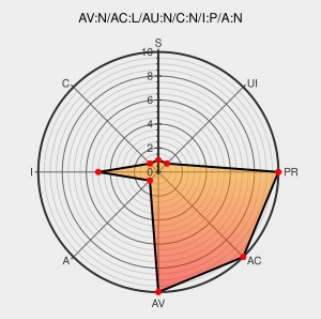
CVE-2004-1756

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 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/resourcelibrary/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

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

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: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:*:*:*:*:*:

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→