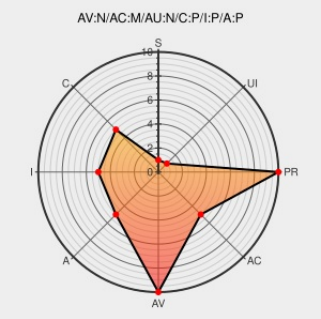
CVE-2005-1380

Published on: 05/02/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1380

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



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

Cross-site scripting (XSS) vulnerability in BEA Admin Console 8.1 allows remote attackers to execute arbitrary web script or HTML via the server parameter to a JndiFramesetAction action.

CVE-2005-1380 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Secunia - Advisories - BEA WebLogic Administration Console Cross-Site Scripting	Vendor Advisory, web.archive.org, text/html	SECUNIA 15128
BEA WebLogic Server And WebLogic Express Administration Console Cross-Site Scripting Vulnerability	Exploit, Vendor Advisory, cve.report (archive), text/html	BID 13400
'Cross Site Scripting in BEA Admin Console' - MARC	marc.info, text/html	BUGTRAQ 20050428 Cross Site Scripting in BEA Admin Console
No Description Provided	Exploit, Vendor Advisory, www.red-database-security.com, text/html	MISC www.red-database-security.com/advisory/bea_css_in_admin_console.html

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF weblogic-jndiframesetaction-xss(20276)
SecurityTracker.com Archives - BEA WebLogic Administration Console Input Validation Hole in 'JndiFramesetAction' Permits Cross-Site Scripting Attacks	Exploit Vendor Advisory securitytracker.com text/html	SECTRACK 1013817
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 15895

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	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	8.1	sp3	All	All
Application	Bea	Weblogic Server	8.1	sp3	express	All
Application	Bea	Weblogic Server	8.1	sp3	win32	All
Application	Bea	Weblogic Server	8.1	sp4	All	All
Application	Bea	Weblogic Server	8.1	sp4	express	All
Application	Bea	Weblogic Server	8.1	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	8.1	sp3	All	All
Application	Bea	Weblogic Server	8.1	sp3	express	All
Application	Bea	Weblogic Server	8.1	sp3	win32	All
Application	Bea	Weblogic Server	8.1	sp4	All	All
Application	Bea	Weblogic Server	8.1	sp4	express	All
Application	Bea	Weblogic Server	8.1	sp4	win32	All

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:8.1:sp3:*:*:*:*:*:*:

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

cpe:2.3:a:bea:weblogic_server:8.1:sp3:win32:*:*:*:*:*:

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:8.1: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:*:*:*:*:*:*:

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:8.1:sp3:*:*:*:*:*:*:

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

cpe:2.3:a:bea:weblogic_server:8.1:sp3:win32:*:*:*:*:*:

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:8.1:sp4:win32:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→