CVE-2009-1974

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-1974
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-14 23:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.3, 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 S

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Bea Product Suite	10.0	mp1	All	All
Application	Oracle	Bea Product Suite	10.3	All	All	All
Application	Oracle	Bea Product Suite	7.0	sp7	All	All
Application	Oracle	Bea Product Suite	8.1	sp6	All	All
Application	Oracle	Bea Product Suite	9.0	All	All	All
Application	Oracle	Bea Product Suite	9.1	All	All	All
Application	Oracle	Bea Product Suite	9.2	mp3	All	All
Application	Oracle	Bea Product Suite	10.0	mp1	All	All
Application	Oracle	Bea Product Suite	10.3	All	All	All
Application	Oracle	Bea Product Suite	7.0	sp7	All	All
Application	Oracle	Bea Product Suite	8.1	sp6	All	All
Application	Oracle	Bea Product Suite	9.0	All	All	All
Application	Oracle	Bea Product Suite	9.1	All	All	All
Application	Oracle	Bea Product Suite	9.2	mp3	All	All

References

Reference	Source	L

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	v
55906	OSVDB	c
Oracle Products Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	s
IBM X-Force Exchange	XF	e
SecurityTracker.com Archives - WebLogic Server Bugs Let Remote Users Gain Access and Modify Data and Deny Service	SECTRACK	v
Oracle WebLogic Server CVE-2009-1974 Remote Vulnerability	BID	v
Oracle Critical Patch Update Advisory - July 2009	CONFIRM	v
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**