CVE-2009-1012

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

Summary

CVE	CVE-2009-1012
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-15 10:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	Unspecified vulnerability in the plug-ins for Apache and IIS web servers in Oracle BEA WebLogic Server 7.0 Gold through 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

Oracle Critical Patch Update Advisory - April 2009
IBM X-Force Exchange
Oracle April 2009 Critical Patch Update Multiple Vulnerabilities
Vulnerabilities - Secunia Research - Vulnerability Information - Secunia.com
Page not found | Oracle
US-CERT Technical Cyber Security Alert TA09-105A -- Oracle Updates for Multiple Vulnerabilities
53765
Oracle WebLogic Server and Portal Bugs Let Remote Users Access and Modify Data and Cause Denial of Service Conditions - SecurityTrack
CVE Program record
NVD vulnerability detail

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**