Patch for Potential Vulnerability in the execution of JSPs outside doc_root

Description of the problem

A potential security vulnerability has been discovered in Oracle JSP releases 1.0.x through 1.1.1 (in Apache/Jserv). This vulnerability permits access to and execution of unintended JSP files outside the doc_root in Apache/Jserv. For example, accessing http://HOST/a.jsp//..//..//..//..//..//../b.jsp will execute b.jsp outside the doc_root instead of a.jsp if there is a b.jsp file in the matching directory.

Products Affected

Oracle8i Release 8.1.7, iAS Release 1.0.2
Oracle JSP, Apache/JServ Releases 1.0.x - 1.1.1

Platforms Affected

Windows NT

Likelihood of Occurrence

Whenever //.. is present in the URI while using Apache/JServ.

Solution

Upgrade to OJSP Release 1.1.2.0.0 which is available on Oracle Technology Network's OJSP web site.

Credits

Oracle Corporation wishes to thank Georgi Guninski for discovering this vulnerability and promptly bringing it to Oracle's attention.