

Vulnerabilities in MODPLSQL

Products

MODPLSQL - ModPL/SQL for Apache, (bundled with iAS, all versions). MODPLSQL is a gateway to call PL/SQL procedures from the web. [Basically, one can write PL/SQL procedures to output HTML that can be read from a browser. MODPLSQL is the piece that communicates with the database, transferring HTML to the browser.]

Platforms Affected

Sun SPARC Solaris 2.6
MS Windows NT/2000 Server
HP-UX 11.0/32-bit

Description

A directory traversal vulnerability, caused by double decoding, may allow read access to files on the server.

A memory boundary write may leave the server vulnerable to a denial-of-service attack and possibly remote execution of code.

Patch Solution

Oracle has fixed these potential security vulnerabilities in the 3.0.9.8.3 release of MODPLSQL, for use with iAS 1.0.2.x.x. Backports to earlier versions of iAS are not offered.

Supported customers may download the release from Oracle's Worldwide Support web site, MetaLink, <http://metalink.oracle.com/>. Activate the "Patches" button to get to the patches web page. Enter patch number 2128936, and activate the "Submit" button.

Credits

Oracle thanks David Litchfield of [NGSSoftware](#) for bringing these vulnerabilities to our attention.