

Patch for Potential Vulnerability in Oracle XSQL Servlet

Description

A potential security vulnerability in Oracle XSQL Servlet has been discovered when using stylesheets as URL parameters which permits the execution of arbitrary Java code on the Oracle 8.1.7.0.0 database server with elevated privileges. This vulnerability was discovered in Oracle8i, Release 8.1.7.0.0, Enterprise Edition running Oracle Internet Application Server (iAS) and XSQL Servlet, Release 1.0.0.0, on MS Windows 2000. It also exists in XSQL releases 1.0.1.0 to 1.0.3.0 on all platforms.

Solution

Oracle has corrected this vulnerability in the new release of XSQL Servlet as well as provided more secure behavior by default. The new release of XSQL Servlet, Release 1.0.4.0, can be obtained from Oracle Technology Network, OTN, http://otn.oracle.com/tech/xml/xsql_servlet. A patch will also be available in the upcoming Oracle8i, Release 8.1.7.1, patch set and available for use with iAS Release 1.0.2.1.

Credits

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