Buffer Overflow Vulnerability in the Oracle8i Listener

Overview
A potential security vulnerability has been discovered in the Oracle8*i* database server listener. This vulnerability may cause a buffer overflow condition that allows remote execution of arbitrary code on the database server under a security context that grants full control of the database services and, on some platforms, full control of the operating system.

Description
The Oracle8*i* database server listener administration and monitoring can be performed by issuing specific requests (commands) to the daemon. Typical requests, such as "STATUS", "PING" and "SERVICES" return a summary of listener configuration and connections. Other requests such as "TRC_FILE", "SAVE_CONFIG" and "RELOAD" are used to change the configuration of the listener. An exploitable buffer overflow occurs when any of the command's arguments contain a very large amount of data.

The Oracle8*i* database server listener daemon runs with "LocalSystem" privileges under Windows NT/2000, and with the privileges of the “oracle” user under Unix. Successful exploitation of this vulnerability may provide an attacker with these respective privileges.

Products Affected
Oracle8*i* database server listener

Platforms Affected
All

Patch Solution
Oracle has fixed this potential security vulnerability in the Oracle9i database server. Oracle is in the process of backporting the fix to supported Oracle8i database server Releases 8.1.7 (patchsets 8.1.7.2 and 8.1.7.3) and 8.1.6 and Oracle8 Release 8.0.6 on all platforms.

Download the patch for your platform from Oracle’s Worldwide Support web site, Metalink, http://metalink.oracle.com. Please check Metalink periodically for patch availability if the patch for your platform is not yet available.

Please see the matrix posted below this Alert for details on patch availability and schedules.

Credits
Oracle wishes to thank COVERT Labs at PGP Security (Network Associates) for discovering this vulnerability and promptly bringing it to Oracle’s attention.