

Oracle SQL*Net and Net8 Malformed Packet Denial of Service Vulnerability

Overview

A potential security vulnerability has been discovered in Net8 (formerly known as SQL*Net).

The Oracle8i database server relies on multiple services for its distributed client server computing functionality. Services that are dependant upon the TNS include the TNS Listener, Oracle Name Service and the Oracle Connections Manager. These servers accept client requests and establish TNS data connections between the clients and the services. A vulnerability exists in the TNS libraries which process Net8 packets. This vulnerability will enable an attacker to mount a denial of service attack against any of the above services by issuing a malformed Net8 connection request.

Products

All releases of the Oracle Listener (database releases Oracle 7.3.x, Oracle 8.0.x, Oracle 8.1.x)

Platforms

All platforms

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 81.7.2 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 would like to thank COVERT Labs at PGP Security (Network Associates) for discovering this potential security vulnerability and promptly bringing it to Oracle's attention.