Patch for Potential Security Vulnerability in Oracle Connection Manager Control

Description

A potential security vulnerability has been discovered in Oracle Connection Manager Control (CMCTL). This vulnerability can force a buffer overflow in CMCTL which can be exploited to gain elevated operating system privilege sets of EGID DBA and EUID ORACLE by an ordinary user supplying command-line arguments to CMCTL. This vulnerability is only possible if SET-GID and SETUID bits, respectively, are set on the CMCTL executable.

Solution

Oracle has fixed this vulnerability in patchsets for Oracle8i, Releases 8.1.6 and 8.1.5, and Oracle8, Releases 8.0.5, 8.0.4 and 8.0.3. The patchsets are available on Oracle's Support Services site, Metalink, http://metalink.oracle.com. All other production releases of the Oracle database server contain this security patch by default.

Credits

Oracle wishes to thank Juan Manuel Pascual Escriba for discovering this security vulnerability and promptly bringing it to Oracle's attention.