Oracle Internet Directory Buffer Overflow Vulnerability

Overview

A potential security vulnerability has been discovered in Oracle Internet Directory (OID).

OID release 2.1.1.0.0 is vulnerable to a potential buffer overflow problem which may permit unauthorized access to the operating system.

Products

Oracle Internet Directory (OID) release 2.1.1.0.0

Platforms

Windows NT (reported)

Workarounds

Oracle recommends the following workarounds to fix the security vulnerability.

On Windows NT

1. From the startup menu, click on “start”, choose “settings”, choose “control panel”
2. Double-click on “services”
3. Select (click on) “OracleDirectoryService_<ORACLE_SID>”
4. Click on “startup “
5. Click on “This Account” radio button
6. Enter the user name and password for another operating system user (or the OID owner account)
7. Click on “OK”
   => this will force OID’s service to run under a different operating system user instead of that of the LocalSystem account.

On Windows 2000

1. From the startup menu, click on "start", choose "settings", choose "control panel"
2. Double click on "Administrative Tools", and then single click on "services"
3. Select (click on) "OracleDirectoryService_<ORACLE_SID>"
4. Click on "Action", "Properties", and then "LogOn"
5. Click on "This Account" radio button
6. Enter the user name and password for another operating system user (or the OID owner account)
7. Click on "OK"
   - ⇨ this will force OID’s service to run under a different operating system user instead of
   - ⇨ that of the LocalSystem account.

On Unix platforms

1. Change the ownership of executable “oidldapd” from root user to the UNIX user who owns the OID installation in the operating system.
2. Set the file permissions on “oidldapd” to 710.
3. Change the ownership of executable “oidmon” from root user to the UNIX user who owns the OID installation in the operating system.
4. Set the file permissions on “oidmon” to 710.
5. Remove (or back up) OID monitor and dispatcher log files before restarting the OID instance.

Patch Solution

Oracle has comprehensively fixed this security vulnerability in the following releases of OID:

1) OID release 3.0.1.1.0 (shipping with Oracle9i) on all Unix platforms
2) OID release 3.0.1.1.0 (shipping with Oracle9i) on Windows
3) OID release 2.1.1.3.0 (shipping with Oracle8i) on Solaris.

Download the patchset for your platform from Oracle's Worldwide Support web site, Metalink, http://metalink.oracle.com.

The patch number for OID release 2.1.1.3.0 is 1888945.
The patch number for OID release 3.0.1.1.0 is 1888998.

NOTE: All pre-3.0.1.x releases of OID including and other than those mentioned above can be satisfactorily protected by following the workarounds described above.

Credits

Oracle would like to thank the University of Oulu Secure Programming Group (OUSPG) and CERT for promptly bringing this potential security vulnerability to Oracle's attention.