Oracle Security Alert #59
Dated: 20 October 2003
Updated: 13 November 2003
Severity: 2

Buffer Overflow in Oracle Database Server Binaries

Description

A potential buffer overflow has been discovered in the “oracle” and “oracleO” (the letter O) binaries of the Oracle Database. A knowledgeable and malicious local user can exploit this buffer overflow to execute code on the operating system hosting the Oracle Database server.

Products Affected

- Oracle 9*i* Database Release 2, Version 9.2.*x*
- Oracle 9*i* Database Release 1, Version 9.0.*x*

Platforms Affected

All supported UNIX and Linux operating system variants.

Required conditions for exploit

A valid account on the operating system hosting the Oracle Database server.

Risk to exposure

The “oracle” and “oracleO” (the letter O) binaries are typically owned by the "oracle” operating system user account and by the "dba" operating system group. A malicious local user (a user defined in the operating system hosting the Oracle Database) can write code that attempts to exploit the buffer overflow in these binaries to run with the privileges of the “oracle” owner and potentially compromise the operating system hosting the Oracle Database server. Unless you connect the Oracle Database directly to the Internet (e.g., no intervening application server or firewall), a remote exploit via the Internet is, in our opinion, unlikely. We strongly recommend that you do not connect the Oracle Database directly to the Internet. However, this vulnerability is susceptible to an insider attack originated on an Intranet if the required conditions for exploit are met.

Oracle is aware of an exploit for this vulnerability.

How to minimize risk

See **Workaround**, below. Follow Oracle’s best practices for database
http://otn.oracle.com/deploy/security/oracle9i/pdf/9ir2_checklist.pdf
http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf
and best practices for operating system security.

Ramification for customer

Oracle recommends that customers review the severity rating for this Alert and patch accordingly. See
http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf
for a definition of severity ratings.

Workaround

Remove the "execute" permission from the operating system group "other" associated with the affected binaries. Perform the following steps:

```
# cd $ORACLE_HOME/bin
# chmod o-x oracle oracleO
```

In addition, verify that only trusted users are in the same group as are the oracle and oracleO binaries.

No other changes are required. For example, do ***not*** remove setuid or setgid from the affected binaries.

NOTE: This workaround protects customers from the potential vulnerability. However, after performing the steps listed above, depending on the configuration of Oracle Net Services, certain users may no longer be able to connect to the Oracle Database. Specifically, if the database is configured to use the bequeath protocol[1], then local users not in the operating system "dba" group will no longer be able to connect to the database. With the workaround applied, ensure that the Oracle Net Listener runs as the same user who owns the oracle binary, or as a user who is a member of the "dba" group. Although this is already the case for a typical installation/configuration, it is not normally required that the user running the listener has these privileges.

For those customers who are unable to implement the workaround as suggested, Oracle recommends applying the patch as soon as it is available.

Patch Availability

Please see Metalink Document ID 256927.1:
http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=256927.1
for the patch download procedures and for the **Patch Availability Matrix** for this Oracle Security Alert.

---

[1]If the client and server exist on the same machine, a client connection can be bequeathed (passed) directly to a dedicated server process without going through the listener. The application initiating the session spawns a dedicated server process for the connection request using the bequeath protocol. This happens automatically if an application is used to start the database on the same machine as the database.

Please review Metalink, or check with Oracle Support Services periodically for patch availability if the patch for your platform is unavailable. Oracle strongly recommends that you backup and comprehensively test the stability of your system upon application of any patch prior to deleting any of the original file(s) that are replaced by the patch.

Modification History

20-OCT-03: Initial release, version 1
22-OCT-03: Identified restrictions of the provided workaround, provided patch details for Linux x86, Oracle 8*i* Database Release 8.1.*x* and earlier proved not vulnerable, version 2
13-NOV-03: Updated with reference to external patch matrix and download procedures, version 3