Revised Security Alert #19
Reference Date: 10/18/01

Oracle Trace Collection Security Vulnerability

Overview
A potential security vulnerability has been discovered in the handling of the environment variable, `ORACLE_HOME`. A buffer overflow is caused when the Oracle binary, `otrcrep`, translates the environment variable, `ORACLE_HOME`, into a string of 240 or more bytes.

The Oracle binary `otrcrep` runs with the `SETUID` `oracle` privileges in the operating system DBA group. The buffer overflow may be exploited by a local user to force overwriting of stack variables in shared memory including the return memory address(es) and thereby execute arbitrary (or specific, malicious) code with the privileges of the `oracle` user and/or the DBA group privileges.

Products
All Oracle database server releases (8.0.x, 8.1.x and 9.0.1)

Platforms
All platforms (except MVS and VMS).

Workaround
On all platforms (except MVS and VMS): If the `ORACLE_HOME` environment variable is being translated into a string of 240 or more bytes, disable Oracle Trace by setting its control parameter in `init<SID>.ora` as follows:

```
oracle_trace_enable=FALSE
```

Additionally, on Unix platforms, change the file permissions on all of the Oracle Trace executables as follows:

```
% chmod -s otrccol otrccref otrcfmt otrcrep
% chmod 751 otrccol otrccref otrcfmt otrcrep
```

Patches
The potential security vulnerability will be code-fixed in the next release of the Oracle database server which is Oracle9*i*, Release 2, only. All other releases of the Oracle database (8.0.x, 8.1.x and 9.0.1) must use follow the workarounds specified above to circumvent the potential security vulnerability.

Credits
Oracle wishes to thank Juan Manuel Pascual EscribÃ for discovering these vulnerabilities and promptly bringing them to Oracle's attention.