**Oracle Security Alert 53**
**Dated: 10 April 2003**
**Severity: 2**

# Report Review Agent (RRA/FNDFS) Vulnerability in Oracle E-Business Suite

## Description

A potential security vulnerability has been discovered in the Oracle E-Business Suite Report Review Agent (RRA) program that allows a knowledgeable and malicious user to spoof requests to gain unauthorized access to application or operating system files.
**Note:** Report Review Agent is also known as the FND File Server (FNDFS).

## Products Affected

- Oracle E-Business Suite 11i, Releases 1 through 8
- Oracle Applications 11.0, All Releases
- Oracle Applications 10.7, All Releases

## Platforms Affected

All

## Required conditions for exploit

The user must have direct access to the TNS Listener port of the RRA/FNDFS host machine without the presence of any kind of intervening firewall and/or application server. In Oracle Applications 10.7 and Oracle Applications 11.0 RRA/FNDFS was installed only on the Concurrent Processing node. In Oracle E-Business Suite 11i it is installed on all Application Tiers.

**Note:** The TNS Listener is a component of Oracle Net services, formerly known as Net8 and SQL*Net.

### Risk to exposure

Risk to exposure is medium due to the reasons listed above.

### How to minimize risk

Follow the best practices for Oracle E-Business Suite: See Metalink note 189367.1 "Best Practices for Keeping Your E-Business Suite Secure" (http://metalink.oracle.com/metalink/plsql/showdoc?db=NOT&id=189367.1).

### Ramification for customer

Oracle recommends applying the applicable patches listed below as soon as possible.

## Severity rating

For a definition of severity rating please refer to:
http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf.

**Patch Information**
The patch fixes the potential security vulnerability by introducing new security procedures for RRA/FNDFS and its clients.

Users of Applications Desktop Integrator (ADI) must apply an additional patch (#**2778660**) so that the ADI client can connect to the upgraded RRA/FNDFS. Without patch 2778660, ADI will no longer be able to connect to the newly upgraded RRA/FNDFS to retrieve concurrent request output files.

The patch README.txt contains the patch application instructions/configuration guide.

**Fixed by**
The security patch is available for the following releases:

- Oracle E-Business Suite 11i, Releases 1 through 8
- Oracle Application 11.0, All Releases

Download this one-off patch from the Oracle Support Services web site, MetaLink (http://metalink.oracle.com).

1. Click on the **Patches** button.
2. Click on the "**New** Metalink Patch Search ".
   If you are not on the "Simple Search" screen, click on the "Simple" button to get to the "Simple Search" screen.
3. Refer to the Patch Availability Matrix below to determine the patch number required.
4. In the "Search By" option select "Patch Numbers(s)" from the drop-down menu, and enter the required patch number in the box.
5. Click on the "Go" button.
6. Select the required platform and language.
7. Click on the "Download" button.
8. Recommended: you can also click on the "View README" button for additional information and instructions.

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.

**Patch Availability Matrix**

| Platforms | 10.7 Release | 11i Releases 1 - 8 | All 11.0 Releases | ADI client |
|---|---|---|---|---|
| Sun Solaris (32-bit) | N/A | 2782945 | 2782950 | N/A |
| IBM AIX 4.3.3 and 5L (32-bit) | N/A | 2782945 | 2782950 | N/A |
| MS Windows NT/2000/XP | N/A | 2782945 | 2782950 | 2778660 |
| HP-UX (32-bit) | N/A | 2782945 | 2782950 | N/A |
| HP Tru64 | N/A | 2782945 | 2782950 | N/A |
| LINUX | N/A | 2782945 | N/A | N/A |
| INTEL SOLARIS | N/A | N/A | 2782950 | N/A |
| SGI-IRIX-64 | N/A | N/A | 2782950 | N/A |

**N/A:** The Oracle E-Business Suite Release/Version is not available for this platform.

**Credits**

Oracle Corporation thanks Stephen Kost of Integrigy Corporation for discovering and bringing this potential security vulnerability to Oracle's attention.

**Modification History**

10-APR: Initial release, version 1