

**Oracle Security Alert 55**  
**Dated: July 23, 2003**  
**Severity: 1**

## **Unauthorized Disclosure of Information in Oracle E-Business Suite**

### **Description**

A potential security vulnerability has been discovered in the Oracle E-Business Suite. A set of JSPs allows users to view product configuration and host system diagnostic information without authentication.

### **Products Affected**

- Oracle E-Business Suite 11i, All Releases
- Oracle Applications, All Releases

### **Platforms Affected**

All platforms.

### **Required conditions for exploit**

A user with HTTP access.

#### **Risk to exposure**

Oracle believes a knowledgeable and malicious user with specialized skills can use the host system diagnostic and product configuration information to exploit Oracle E-Business Suite.

#### **How to minimize risk**

There are no workarounds that directly address the potential security vulnerability, but a patch is available (see below). Oracle strongly recommends that customers follow best practices for Oracle E-Business Suite, Note 189367.1 "Best Practices for Keeping Your E-Business Suite Secure" available at <http://metalink.oracle.com>.

#### **Ramification for customer**

Customers are vulnerable unless the patch fix is applied.

Oracle strongly recommends that customers review the severity rating for this Alert and patch accordingly. See [http://otn.oracle.com/deploy/security/pdf/oracle\\_severity\\_rating\\_s.pdf](http://otn.oracle.com/deploy/security/pdf/oracle_severity_rating_s.pdf) for a definition of severity ratings.

### **Patch Information**

The patch disallows standalone access to AOL/J Setup Test JSPs and forces users to sign-on using a secure application schema login.

*Note:* The patch must be applied to all platforms and across all releases of Oracle E-Business Suite Release 11i and Oracle Applications.

**Fixed by**

Obtain and install the correct Mandatory Applications Security Patch for your release of E-Business Suite:

- Oracle E-Business Suite 11i, All Releases
- Oracle Applications, 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 Search" button.
3. Input the bug number **2939083** on the "Search by Patch Number" box.
4. Click Go.
5. Select the patch for the appropriate product version.
6. Click Download.

**Credits**

Oracle Corporation thanks Stephen Kost of Integrigy Corporation for discovering and promptly bringing this potential security vulnerability to Oracle's attention. The Integrigy alert is available at <http://www.integrigy.com/alerts.htm>.

**Modification History**

23-JUL-03: Initial release, version 1