

# Oracle E-Business Suite Flaw



---

**CVE -2008- 5446 Sensitive Information Disclosure**

**Date: 13 January 2009**

---

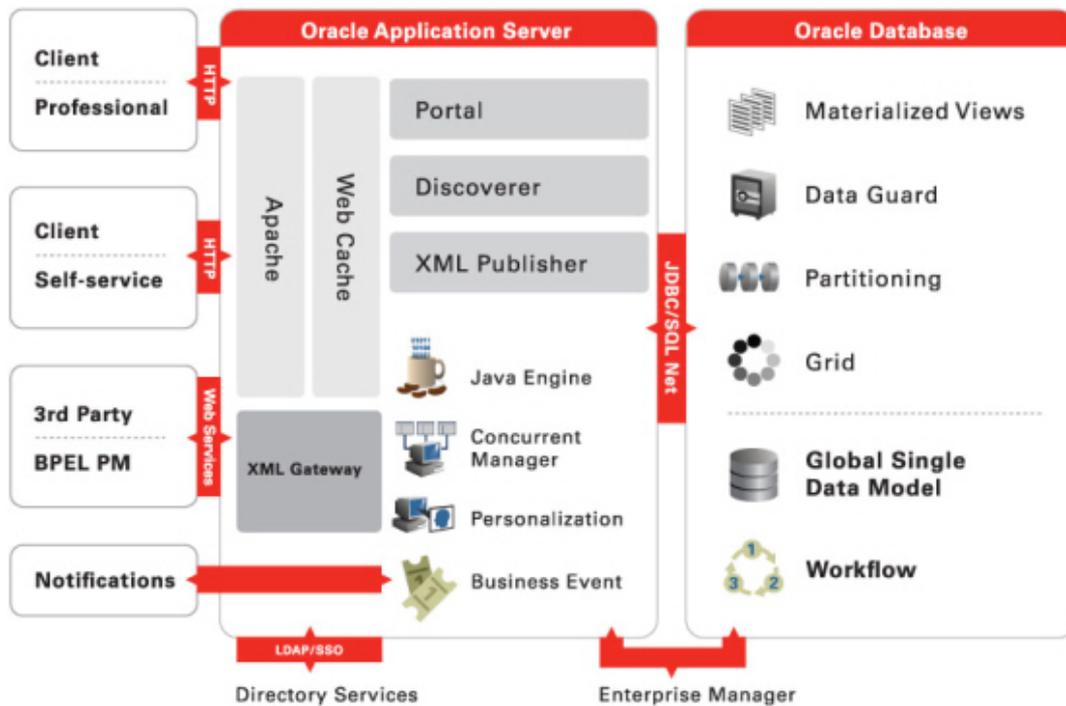
---

Aditya K Sood aka 0kn0ck , <http://www.secniche.org> | [adi\\_ks \[at\] secniche.org](mailto:adi_ks@secniche.org)

---

*2008 All Rights Reserved. SecNiche makes no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, photocopying, recording or otherwise, without prior written consent of SecNiche. While every precaution has been taken in the preparation of this publication, this publication and features described herein are subject to change without notice.*

**The E-Business Suite Overview:**



**Oracle E-Business Suite Sensitive Information Disclosure Vulnerability**

The oracle E Business including applications like I-Recruitment etc is vulnerable to flaw which leads to sensitive information disclosure about the deployment of oracle application and server in a production environment. The flaw persists in the E Business suite designed code which allows malicious user to steal sensitive information through "About Us Page" (shipped with E Business Suite) by allowing guest access. In addition to this a straight forward access is granted to attacker to steal all the information which provide potential attack surface for conducting stringent attacks.

The severity gets higher because the type of information is revealed. This can be structured over two end points as:

1. If an application is hosted on internet with external interface.
2. If an application is hosted in organization production environment.

Both cases lead to high risk.

The type of information that can be extracted is:

- [1] Personalization Info: Application information
- [2] Page Context: Information about the instance of running page and environment.
- [3] Technology Component: The technology related information.
- [4] Java System Properties: The configuration of Java Virtual Machines
- [5] Profiles: System Profile Specific Information
- [6] Patches: The Latest Patches Applied to the System

[Check Appendix for Detail Snapshots]

**This vulnerability has been noticed on all versions of Oracle E Business Suite including version 12.**

**Oracle Security Team View**

*"The investigation of the issue you originally reported indicated the problem is in code that underlies all E-Business Suite applications in a common framework layer called Oracle Applications Framework (OAF). Any E-Business product that uses this functionality is potentially affected by the problem you found. Development have created a fix for this issue, and it will be tested and back port to other supported versions before it is released in a Critical Patch Update. "*

**Oracle Critical Patch updates:**

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2009.html>

**Oracle Credited SecNiche Security for finding this vulnerability.**

**Refer to:**

**Security Administration**

[http://download.oracle.com/docs/cd/B40089\\_10/current/acrobat/120sasg.pdf](http://download.oracle.com/docs/cd/B40089_10/current/acrobat/120sasg.pdf)

## Appendix

### Critical Information Disclosed:

#### [1] Personalization Info: Application information

Home >  
 About Page: iRecruitment Visitor Home Page

Printable Page Generate Bug Report

Page Personalization Page Context Technology Components Java System Properties Profiles Patches

**Effective Personalizations** Manage Personalization List

**iRecruitment Visitor Home Page**  
 /oracle/apps/per/irc/candidateSelfService/webui/VisHomePG

Level	Value	Customized Elements	Last Updated	Default View
function	IRC_VIS_HOME_PAGE	MainLinksList - F9_IRC_EXT_LINK_1	2008-01-16	
responsibility	23350 - IRC_EXT_CANDIDATE - iRecruitment External Candidate	SsoLogin - ReviewBenefits - AdvancedSearch - SalesJobs - LeftFlexLayout - flexibleLayout_0_1185824636359 - ContractJobs - LeftTopFlexLayout - LeftBottomFlexLayout - flexibleLayout_0_1185824710177 - flexibleLayout_1_1185824710178 - JobSearchFlexContent	2008-01-16	
site	0	ReviewBenefits - lynx_cospr_hrevent - MainLinksFlexContent	2008-04-10	

**Shared Region: Job Search**  
 /oracle/apps/per/irc/candidateSelfService/webui/VisHmeJobSchSCRN

Level	Value	Customized Elements	Last Updated	Default View
responsibility	23350 - IRC_EXT_CANDIDATE - iRecruitment External Candidate	vis.JobSeachButtonBar.VisAdvancedSearchBtn	2008-01-07	
site	0	ProfessionalAreaCode - DerivedLocaleLocation	2008-01-07	

#### [2] Page Context: Information about the instance of running page and environment.

About Page: iRecruitment Visitor Home Page

Printable Page Generate Bug Report

Page Personalization Page Context Technology Components Java System Properties Profiles Patches

Database /d01/applmgr/prodappl/fnd/11.5.0/secure/PROD\_lynxrecruit\_vcosxaah0a/prod.dbc  
 Host Name ( ) JDBC Port (1521) SID (PROD)  
 User Name GUEST  
 Application 800 - PER - Human Resources  
 Responsibility 23350 - IRC\_EXT\_CANDIDATE - iRecruitment External Candidate  
 Organization 2 -  
 Language en\_US  
 Server Timezone  
 Client Timezone  
 JVM Default Timezone sun.util.calendar.ZoneInfo[id="America/New\_York",offset=-1800000,dstSavings=3600000,useDaylight=true,transitions=235,lastR

**Security**

Item	Function	Rendered
pageLayout: iRecruitment Visitor Home Page	IRC_VIS_HOME_PAGE	\${oa.FunctionSecurity.IRC_VIS_HOME_PAGE}
link: New Jobs (Last 7 days)		\${oa.FunctionSecurity.IRC_VIS_HOME_NEW_JOBS}
link: Post Your Resume		\${oa.FunctionSecurity.IRC_EXT_VIS_LINK_CANDHOME}
rawText: <div class="OrainstructionText"> If you...		\${oa.FunctionSecurity.IRC_EX_EMP_REGISTRATION}

**Menu**

TIP It displays responsibility menu with current selected menu / function underlined.

Expand All | Collapse All

**[3] Technology Component: The technology related information.**

About Page: iRecruitment Visitor Home Page

Printable Page   Generate Bug I

Page	Personalization	Page Context	Technology Components	Java System Properties	Profiles	Patches
<b>Product/Component</b>		<b>Version</b>				
OA Framework	11.5.10.5RUP					
Oracle Applications Extension	9.0.3.8.13 - build 1541					
Business Components	9.0.3.13.97					
UIX (Cabo)	2_2_24_1					
BiBeans Runtime	3.1.0.80 nondebug BI Beans 3.1.0.x					
MDS	9.0.5.4.89_555					
XML	Oracle XDK Java 9.0.4.0.0 Production					
AOLJ	Applications Object Library, Core Java Roll Up Patch J					
Servlet	2.2					
Java	1.4.2_04					
JDBC Driver	9.2.0.6.0					
Database	Oracle9i Enterprise Edition Release 9.2.0.8.0 - Production					
Operating System	Linux 2.6.9-55.0.2.ELsmp					
Browser	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.16) Gecko/20080702 Firefox/2.0.0.16					

Printable Page   Generate Bug I

Return to Page: iRecruitment Visitor Home Page

Ink Backlot | Diagnostic

**[4] Java System Properties: The configuration of java**

About Page: iRecruitment Visitor Home Page

Printable Page   Generate Bug I

Page	Personalization	Page Context	Technology Components	Java System Properties	Profiles	Patches
<b>System Property</b>		<b>Value</b>				
APPLRGF	/d01/applmgr/prodcomn/rgf/PROD_lynxrecruit_vcosxaah0a					
APPL_TOP	/d01/applmgr/prodappl					
APPS_JDBC_DRIVER_TYPE	THIN					
BNEDBCFILE	/d01/applmgr/prodappl/fnd/11.5.0/secure/PROD_lynxrecruit_vcosxaah0a/prod.dbc					
CLIENT_PROCESSID	23472					
COMMON_TOP	/d01/applmgr/prodcomn					
DBCFILE	/d01/applmgr/prodappl/fnd/11.5.0/secure/PROD_lynxrecruit_vcosxaah0a/prod.dbc					
DBCLocation	/d01/applmgr/prodappl/fnd/11.5.0/secure/PROD_lynxrecruit_vcosxaah0a/prod.dbc					
DB_HOST	vcosxaah0a.flyfrontier.com					
DB_PORT	1521					
DebugLevel	5					
DebugOutput	/d01/applmgr/prodcomn/conf/PROD_lynxrecruit_vcosxaah0a/AS/Adobe/Apache/Apache/logs/debug.log					
DebugSwitch	OFF					
EXTERNAL_URL	https://lynxrecruit.flyfrontier.com					
FND_SECURE	/d01/applmgr/prodappl/fnd/11.5.0/secure/PROD_lynxrecruit_vcosxaah0a					
FND_TOP	/d01/applmgr/prodappl/fnd/11.5.0					
HTTPClient.Modules	HTTPClient.RetryModule HTTPClient.RedirectionModule HTTPClient.AuthorizationModule HTTPClient.I					
HZ_DNB_CONFIG_DIR	/d01/applmgr/prodcomn/java/com/dnb/gaconfig/					
IMT_COM_PROPERTY_FILE	/d01/applmgr/prodappl/imt/11.5.0/admin/scripts/imtjserv.properties					

Done lynxrecruit.flyfro

[5] Profiles: System profile specific information

About Page: iRecruitment Visitor Home Page Printable Page

Page Personalization Page Context Technology Components Java System Properties Profiles Patches

Query Profile

Expand All Collapse All

Focus Name	Code	User	Responsibility	Application	Site
Profiles that affect OA Framework application behavior					
Release-Specific Behavior					
Preferences					
Web Server					
Session					
Logging / Diagnostics					
Performance					
Personalization					
Passivation					
Application Module Pooling					
Branding					
Partial Page Rendering (PPR)					
Home Page					
Look-and-Feel					
Page Access Tracking					

[6] Patches: The patches applied

About Page: iRecruitment Visitor Home Page

Page Personalization Page Context Technology Components

Applied Patches:PROD

Previous 1-10 Next 10

Patch	Application	Abstract	Type	Completion Date
6208000			ONE-OFF	16-Jan-2008
6372555			ONE-OFF	28-Dec-2007
6708222			ONE-OFF	28-Dec-2007
6399200			ONE-OFF	28-Dec-2007
6399900			ONE-OFF	28-Dec-2007
6628358			ONE-OFF	28-Dec-2007
6701332			ONE-OFF	28-Dec-2007
6399100			ONE-OFF	24-Nov-2007
115GLOBAL			ONE-OFF	28-Dec-2007
6133333			ONE-OFF	24-Nov-2007

Previous 1-10 Next 10

Included Patches

Patch Number

This is most critical information extracted against any oracle based deployed application.