Whitepaper Advisory – SNS09-01

Oracle E-Business Suite Flaw

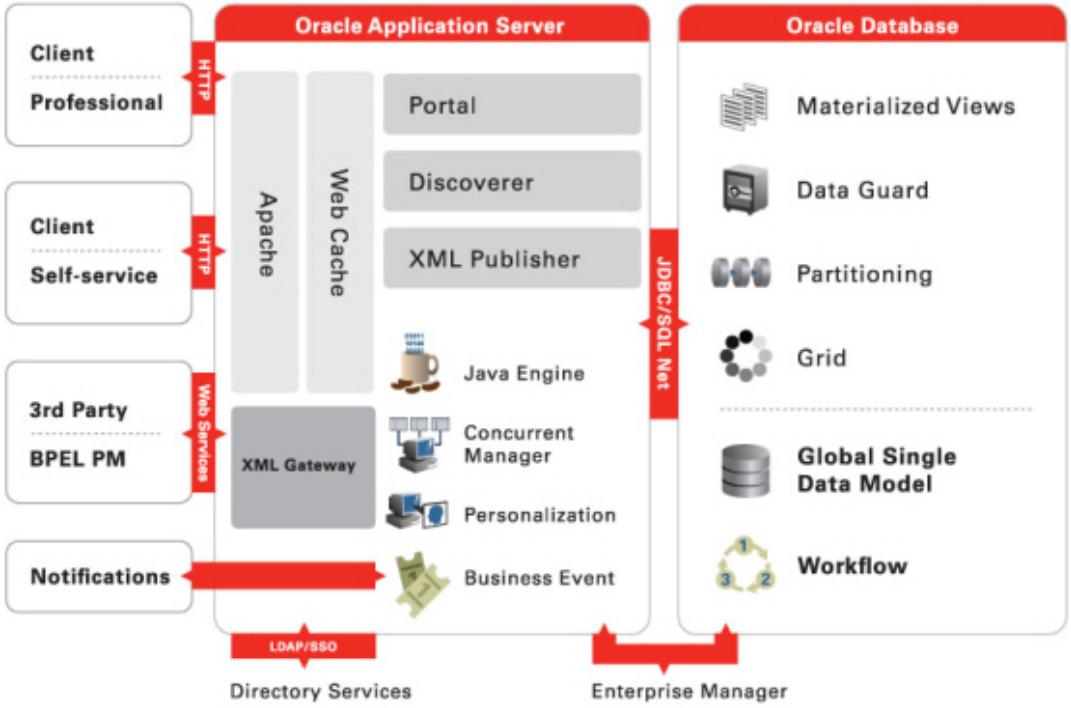
CVE -2008- 5446 Sensitive Information Disclosure

Date: 13 January 2009

Aditya K Sood aka 0kn0ck , http://www.secniche.org | adi_ks [at] secniche.org

---

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:

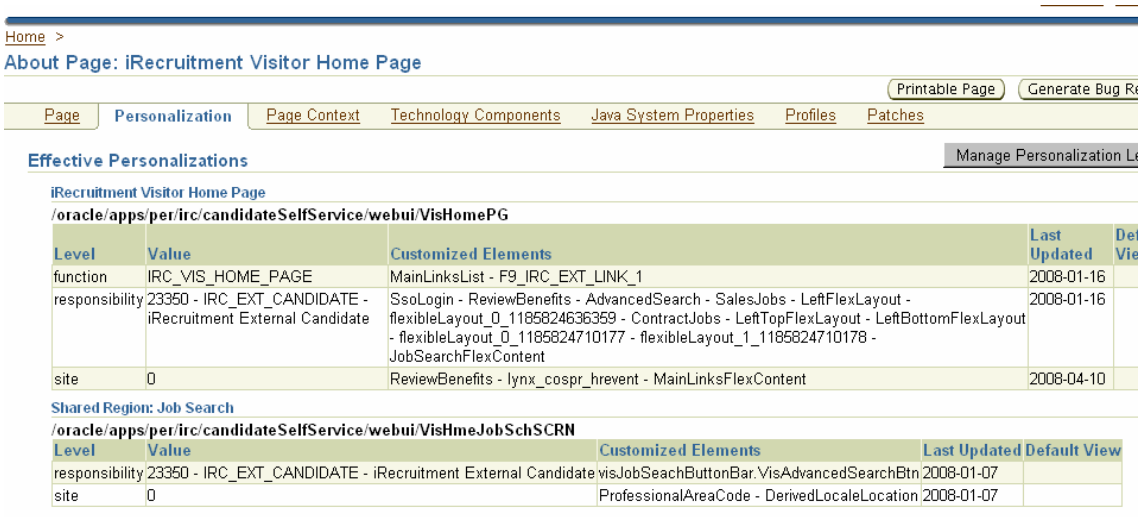
Security Administration

http://download.oracle.com/docs/cd/B40089_10/current/acrobat/120sasg.pdf

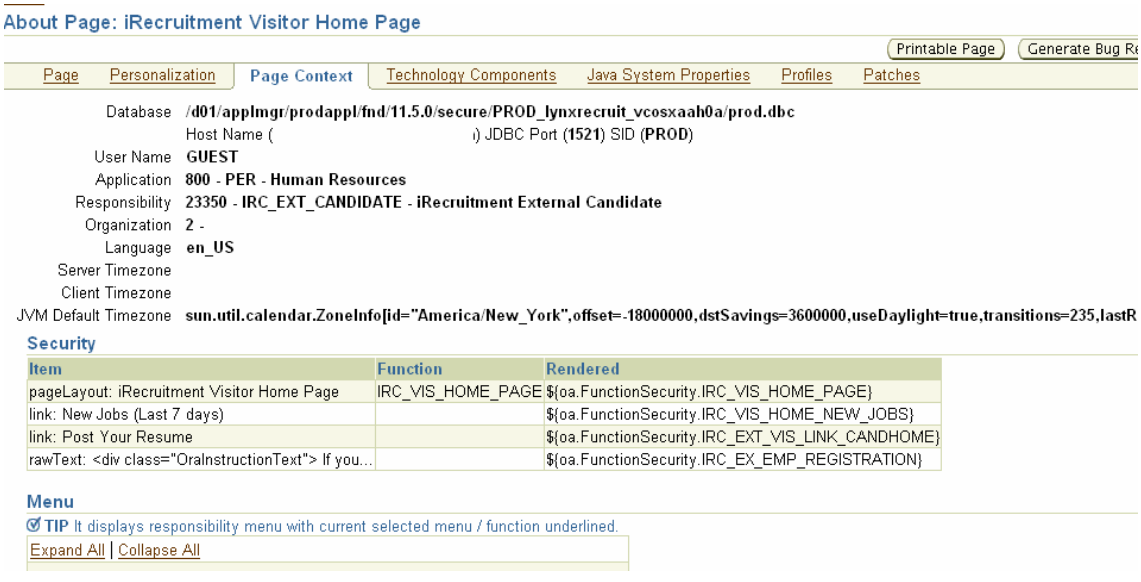
Appendix

Critical Information Disclosed:

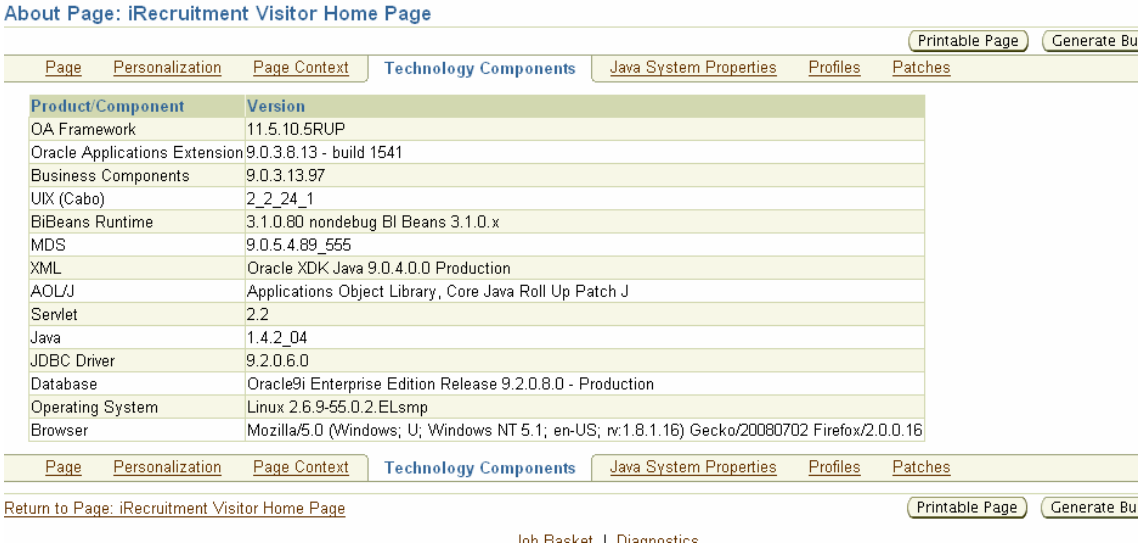
[1] Personalization Info: Application information



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



[3] Technology Component: The technology related information.



About Page: iRecruitment Visitor Home Page

Printable Page | Generate Bu

Page | Personalization | Page Context | **Technology Components** | Java System Properties | Profiles | Patches

Product/Component	Version
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
AOL/J	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

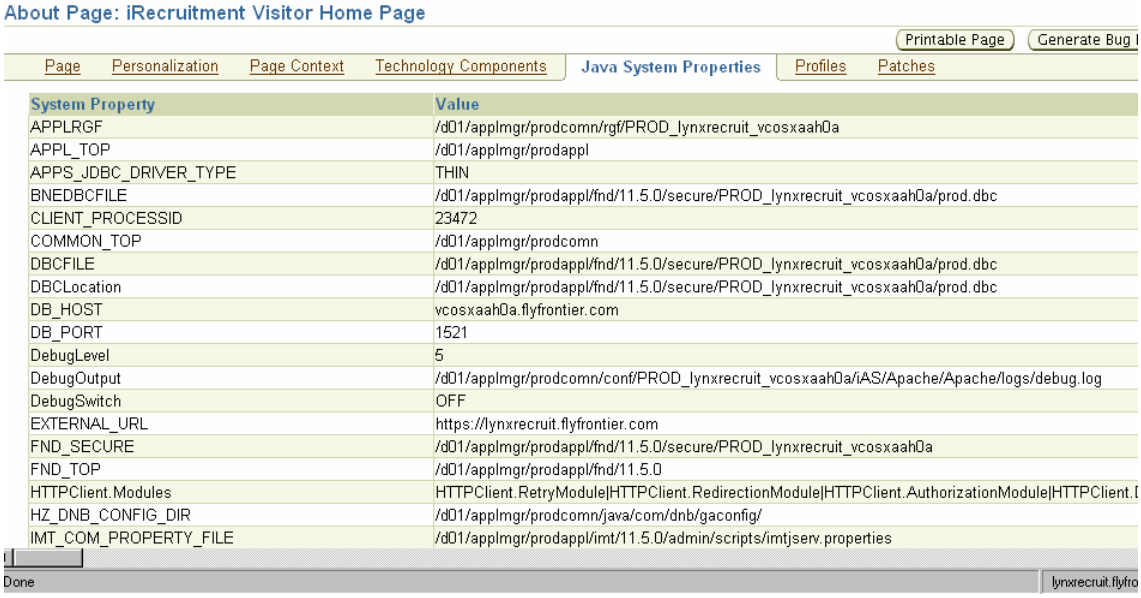
Page | Personalization | Page Context | **Technology Components** | Java System Properties | Profiles | Patches

Return to Page: iRecruitment Visitor Home Page

Printable Page | Generate Bu

Job Basket | Diagnostics

[4] Java System Properties: The configuration of java



About Page: iRecruitment Visitor Home Page

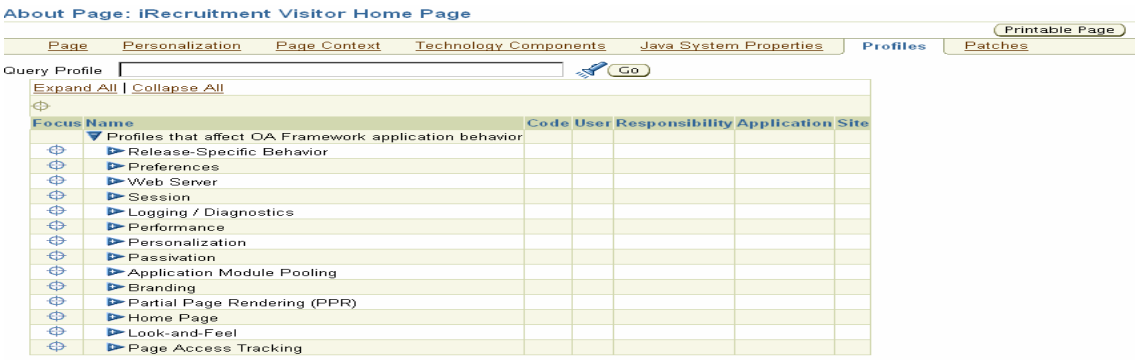
Printable Page | Generate Bug

Page | Personalization | Page Context | Technology Components | **Java System Properties** | Profiles | Patches

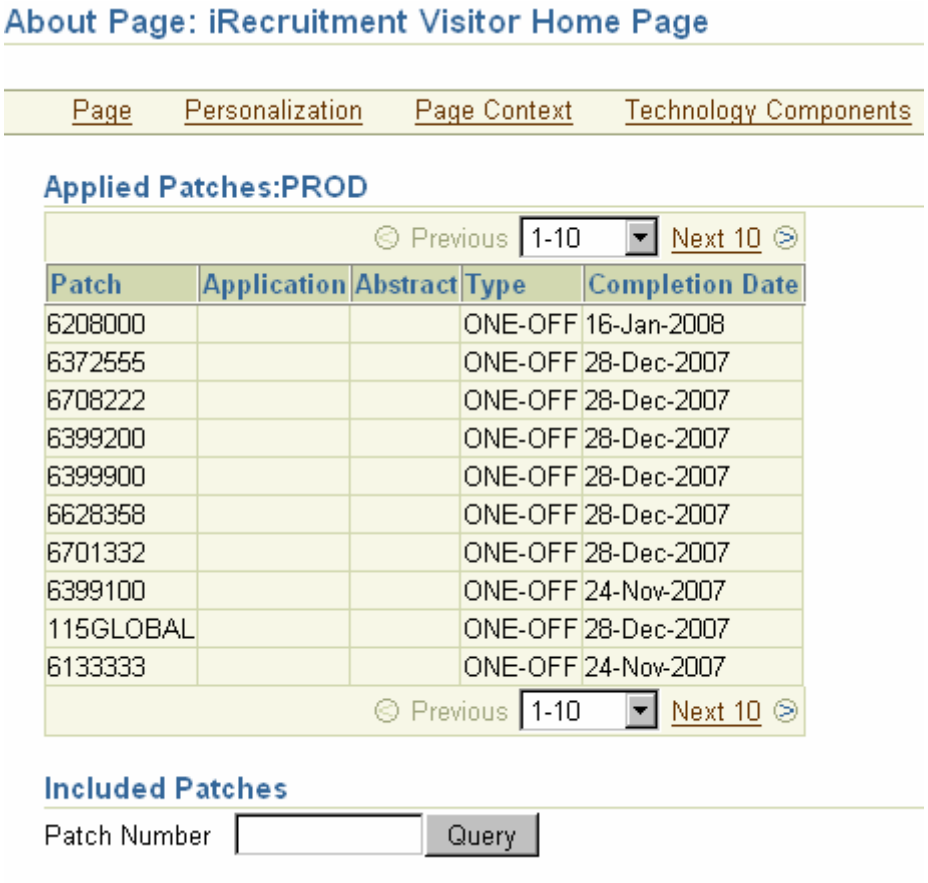
System Property	Value
APPLRGF	/d01/applmgr/prodcomn/rgf/PROD_lynxrecruit_vcosxaah0a
APPL_TOP	/d01/applmgr/prodappl
APPS_JDBC_DRIVER_TYPE	THIN
BNEDBCFILE	/d01/applmgr/prodappl/fnd/11.5.0/secure/PROD_lynxrecruit_vcosxaah0a/prod.dbc
CLIENT_PROCESSID	23472
COMMON_TOP	/d01/applmgr/prodcomn
DBCFILE	/d01/applmgr/prodappl/fnd/11.5.0/secure/PROD_lynxrecruit_vcosxaah0a/prod.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/iAS/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.[
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



[6] Patches: The patches applied



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