Oracle Applications

INTEGRIGY

February 24, 2006

Security Analysis

Diagnostics Support Pack February 2006 Patch

Oracle E-Business Suite Impact

Overview

Oracle Corporation released the "Diagnostics Support Pack February 2006 with Oracle Diagnostics 2.3 RUP A" on February 23, 2006, which is an upgrade to the Oracle E-Business Suite diagnostics and includes a number of security fixes. Due to the number of security fixes included in this patch, Oracle is advising customers to apply this patch and that these security fixes will also be included in the next quarterly Critical Patch Update (April 18, 2006).

Oracle Diagnostics is a troubleshooting feature of the Oracle E-Business Suite 11i that allows system administrators and other users to execute technical and functional tests on the configuration and setup of the application. These tests cover a wide range of functionality from the application server setup to functional tests in modules such as General Ledger and Human Resources

There exist a number of high risk security vulnerabilities in the Oracle Diagnostics web pages and Java classes. The most significant issue with the Oracle Diagnostics is that some of the diagnostics can be executed without any authentication and it is possible to configure the diagnostics to be unrestricted. Also, several permission issues and SQL injection vulnerabilities are fixed by the patch.

It is standard procedure for Oracle to include security fixes in upgrades such as this one prior to the release of the security fixes in a Critical Patch Update, however, Oracle has not previously provided customers a notification that security fixes were included. We believe Oracle is encouraging customers to upgrade to the latest support diagnostics as a way to improve technical support and by highlighting a security risk will accelerate the adoption of the diagnostics patch.

Affected Oracle Products

This patch and related security vulnerabilities have no impact on other Oracle products including but not limited to the Oracle Database, Oracle Application Server, and Oracle Collaboration Suite.

Components of the new Oracle Diagnostics module (IZU) have been available in Oracle Applications since 11.5.3 when the diagnostic framework was introduced and named Oracle Diagnostics. Oracle Diagnostics was initially part of the CRM Technology Foundation (JTT) and CRM Data Model (JTF) modules.

	Oracle Diagnostics Installed Version			
	< 2.0	2.0	2.1	2.2
11.5.10 CU2				X
11.5.10 CU1				X
11.5.10				X
11.5.9			X	
11.5.8		X		
11.5.7	X			
11.5.6	X			
11.5.5	X			
11.5.4	X			
11.5.3	X			
FND.H				X
OAM.H				X
OAM.G			X	
JTT.E				X
JTT.D		X		

Assessment of Vulnerabilities

The diagnostics tools and functions within Oracle Applications have been the source of numerous security vulnerabilities over the years and are fixed in a number of Security Alerts and Critical Patch Updates including Oracle Security Alert #55 and Critical Patch Updates April 2005 and July 2005.

The most significant security change in this patch is the implementation of function security, which limits access to the diagnostics tests. Prior to this patch, some of the diagnostics tests could be accessed without even logging into Oracle Applications. Also, many implementations have enabled unrestricted access to the diagnostics by setting `DIAGNOSTICS_SECURITY_SWITCH=OFF` in the `jserv.properties` file. In Oracle Diagnostics 2.3, this security switch is removed and access is required to execute any diagnostic.

An exact list of diagnostic tests and sample output can be found in Metalink Note ID 179661.1 “Applications Support Diagnostic Tools”.

In addition, several permission issues and SQL injection vulnerabilities are also corrected by the patch. An example of a permission issue is that any user could retrieve diagnostic test log files for other users.

The Oracle Diagnostics can be accessed with the following URL –

http://<host>:<port>/OA_HTML/jtfqalgn.htm

If a login page is displayed, then Oracle Diagnostics 2.3 is already installed. Otherwise, Oracle Diagnostics 2.2 or earlier is installed.

Patch Analysis

In addition to fixing a number of security bugs, this patch actually enhances and extends the capabilities of the Oracle Diagnostics framework.

The following documents on Oracle Metalink provide information on Oracle Diagnostics and detailed installation instructions for Oracle Diagnostics 2.3 –

167000.1 – Oracle Diagnostics Support Pack Installation Guide
342561.1 – Oracle Diagnostics 2.3
342459.1 – Oracle Diagnostics Overview

Two patches are required for Oracle Diagnostics. The first patch registers the new product Support Diagnostics (IZU) and the second patch installs Oracle Diagnostics 2.3. The only significant perquisite is that AutoConfig enabled implementations require AD.I.2.

3636980 – Support Diagnostics (IZU) Patch for AD Splice

Patch 3636980 creates the new product Support Diagnostics (IZU). This patch should not have any impact as it only installs the new product IZU (APP_TOP directory, database schema, and registers it in the necessary files and tables).

- For AutoConfig enabled implementations, AD.I.2 is required.
- The tablespace names defined in the `newprods.txt` file must be changed prior to running ADSPLICE.
- The password must be changed for the IZU database account after applying the patch -- use FNDCPASS to change the password.

4870323 – Oracle Diagnostics 2.3 RUP A

Patch 4870323 only updates files and database objects associated with the Diagnostics framework in Support Diagnostics (IZU) and the CRM Data Model (JTF). There should be no functional impact or testing required outside of testing Oracle Diagnostics. The perquisites for this patch are at least 11.5.4, FND.D, and JTT.D.

From the Patch 4870323 Readme, Step 3 “Removing Legacy Files” must be performed and is critical to resolving potential security vulnerabilities, including removing the DIAGNOSTIC_SECURITY_SWITCH setting.

In order to now access Oracle Diagnostics, access must be setup using either a custom responsibility or adding the menu and functions to an existing responsibility. See Metalink Note ID 358831.1 “Diagnostics Responsibility Configuration” for more information.

Testing

No functional testing is required, since the patches only impact Oracle Diagnostics (IZU and JTF).

Oracle Diagnostics should be tested to verify proper functioning and that access is limited.

Alternative Workaround

If the Oracle Diagnostics 2.3 RUP A patch can not be applied, it is possible to block access to many of the Oracle Diagnostics web pages and also to remove old versions of the Oracle Diagnostics. This workaround is also recommended for all Internet facing Oracle Applications 11i application servers, especially for application servers not configured using Metalink Note 287176.1 "Oracle E-Business Suite 11i Configuration in a DMZ".

Block Access

If the application server was implemented using Metalink Note 287176.1 "Oracle E-Business Suite 11i Configuration in a DMZ", verify that the URL Firewall rules do not allow access to URLs that begin with "/OA_HTML/jtfqa".

For all other Oracle Applications 11i application servers, it is possible to block most access to all versions of Oracle Diagnostics by using a rewrite rule that blocks access to the majority of the Oracle Diagnostics Java Server Pages (JSP). Almost all the Oracle Diagnostics JSPs begin with "jtfqa". Create a rewrite rule in the httpd.conf file or similar file to block all URLs beginning with "/OA_HTML/jtfqa". For AutoConfig enabled implementations, see Metalink Note 270519.1 for information on how to customize AutoConfig files.

Remove Legacy Oracle Diagnostics Files

1. Remove the directory and all files under `$OA_HTML/bin/supp`. This directory was the default location for early versions of the Oracle diagnostic scripts. This directory most likely exists in upgraded Oracle Applications implementations, especially from early 11i versions (i.e., 11.5.1 – 11.5.3).
2. Find and remove the file `support_addon.zip`. This file most likely resides in the $JAVA_TOP directory, but may exist in other locations.
3. Remove the classpath entry for `support_addon.zip` from the `jserv.properties` configuration file. If AutoConfig is enabled, this entry may reside in a `#Begin/End Customizations` block.
4. Remove the entry for `DIAGNOSTICS_SECURITY_SWTICH` from the `jserv.properties` configuration file. If AutoConfig is enabled, this entry may reside in a `#Begin/End Customizations` block.

About Integrigy Corporation

Integrigy Corporation is a leader in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. AppDefend is an intrusion prevention system for Oracle Applications and blocks common types of attacks against application servers. Integrigy Consulting offers security assessment services for leading ERP and CRM applications.

AppSentry and AppDefend have been updated to detect and/or block the vulnerabilities addressed in the Oracle patch "Diagnostics Support Pack February 2006 with Oracle Diagnostics 2.3 RUP A".

For more information, visit www.integrigy.com

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681 USA
888/542-4802
www.integrigy.com