January 25, 2015

Oracle Security Analysis

Oracle E-Business Suite SYS.DUAL PUBLIC Privileges Security Issue (CVE-2015-0393)

Summary

Oracle E-Business Suite environments may be vulnerable due to excessive privileges granted on the SYS.DUAL table to PUBLIC. This security issue has been resolved in the January 2015 Oracle Critical Patch Update (CPU) and has been assigned the CVE tracking identifier CVE-2015-0393. The problem may impact all Oracle E-Business Suite versions including 11.5, 12.0, 12.1, and 12.2. Recent press reports have labeled this vulnerability as a “major misconfiguration flaw.” The security issue is actually broader than just the INDEX privilege that is being reported in the press and there may be at least four independent attack vectors depending on the granted privileges.

Integrigy estimates less than 10% of all Oracle E-Business Suite environments are vulnerable to this security issue based on our previous assessments of production environments. Integrigy has been tracking this issue and checking for it in Oracle E-Business Suite environments since 2007 – we have only identified the problem during a small fraction of our assessments. Vulnerable environments have included 11.5.10.2, 12.0.x, and 12.1.3 and most Oracle E-Business Suite Vision demonstration environments. Most likely, the problem is introduced into the environment during a maintenance operation as it is not found in a fresh installation of the Oracle E-Business Suite. See the Background section of this document of more information.

Validation

To validate if your environment is vulnerable to this issue, execute the following SELECT statement as a privileged user to view the grants –

```
SELECT * FROM sys.dba_tab_privs
WHERE owner = 'SYS' AND table_name = 'DUAL';
```

This query should return only a few grants and all should have only the SELECT privilege. All SELECT privileges are appropriate and no action is required.

If the query returns any rows with a privilege other than SELECT (sometimes up to 20), the environment may be vulnerable depending on the privileges. The “INDEX” and “ALTER” privilege may allow an attacker to escalate privileges. All privileges other than SELECT should be revoked.

SOLUTION

All privileges other than SELECT should be revoked from the SYS.DUAL table. These privileges may be revoked manually or through an update provided in the January 2015 Critical Patch Update for the Oracle E-Business Suite.

Revoking these grants must be done during application maintenance as many Oracle E-Business Suite packages will become invalid and will need to be recompiled using the adadmin utility before restarting the application.

ORACLE CRITICAL PATCH UPDATE (CPU) JANUARY 2015

The January 2015 Oracle CPU patches for Oracle E-Business Suite include a new Oracle E-Business Suite database package in the APPS schema that removes unnecessary grants from PUBLIC on the SYS.DUAL table. Apply the appropriate patch as outlined in My Oracle Support Note ID 1935468.1. Oracle has released additional information in “January 2015 Critical Patch Update: Additional Information About Vulnerability CVE-2015-0393” My Oracle Support Note ID 1964164.1. The key point of Note 1964164.1 is that the database patch 19393542 must be applied by revoking any unnecessary privileges.

STEP 1

Apply Oracle Database patch 19393542. If this patch is not applied first, “subtle timestamp corruptions” may occur in the database when the grants on SYS.DUAL are revoked.

STEP 2

For 11i only, the script **adgrants.sql** script located in the admin directory of the patch must be run before applying the CPU patches.

STEP 3

Apply the appropriate Oracle E-Business Suite CPU patches outlined in Note 1935468.1. The script **$AD_TOP/patch/115/sql/ADFIXUSER.sql** is run by **adpatch** which removes the unnecessary grants.

STEP 4

For R12 only, the CPU patch has manual instructions to run the **adgrants.sql** script. This script will create the AD_ZD_SYS package in the SYS schema. AD_ZD_SYS has a single procedure FIX_SYSUSER, which revokes unnecessary grants on SYS.DUAL.

STEP 5

Validate all unnecessary grants have been removed using the SQL provided in the Validation section of this document.

MANUAL REVOKE

STEP 1

Apply Oracle Database patch 19393542. If this patch is not applied first, “subtle timestamp corruptions” may occur in the database.

STEP 2

The unnecessary grants also may be removed manually. Use the following SQL statement to generate a list of revoke statements –

```
SELECT 'revoke ' || privilege || ' ON sys.dual FROM public;' "SQL"
FROM sys.dba_tab_privs
WHERE owner = 'SYS' AND table_name = 'DUAL'
AND grantee = 'PUBLIC' AND privilege != 'SELECT';
```

STEP 3

Validate all unnecessary grants have been removed using the SQL provided in the Validation section of this document.

STEP 4

Check for invalid database objects and compile as necessary using adadmin.

Background

The exact origin of the non-SELECT grants on SYS.DUAL is unknown, however, these grants only exist in a fraction of all Oracle E-Business Suite installations. These grants do not occur in fresh installations of the application, therefore, are most likely introduced by either a patch or maintenance process. Based on information contained in Oracle Bug 13704367 (February 2012), we believe the older versions of the adadmin utility are responsible and create the grants when the Maintain Database Objects -> Check DUAL Table option is executed. This is not a frequently executed option, which may explain why only some Oracle E-Business Suite environments are vulnerable.

In 2007, Oracle fixed the issue for 11i (Oracle Patches 5759020, 5989593) by including in the **adgrants.sql** script a statement to revoke all grants on sys.dual and then specifically granting only SELECT to public. However, due to issues encountered by customers, this was commented out shortly thereafter and never subsequently fixed. This still appears commented out in all versions of the adgrants.sql script. The following comment in included in the 11i version of **adgrants.sql** –

```
-- Bug 5989593:
-- If ATG RUP5 includes this call to "revoke all from public",
-- they may have to explicitly tell customers to "run adadmin/compile invalid"
-- every time they run adgrants.sql.  In addition, 'evaluation context'
-- objects will not be compiled (there is a security bug that was filed for
-- this issue).
-- Until we find a proper solution for "revoke all from public", we should
-- remove this call from adgrants.sql and adgrants_nt.sql from the 11i
-- versions.
--
-- commenting out this code snippet for now...
--
-- begin
--    execute immediate 'revoke all on sys.dual from public';
--    execute immediate 'grant select on sys.dual to public';
-- exception
--    when others then
--       raise;
-- end;
```

References

- Oracle Critical Patch Update January 2015 Advisory, 20 January 2015, http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
- Oracle E-Business Suite Releases 11i and 12 Critical Patch Update Knowledge Document (January 2015), 20 January 2015, My Oracle Support Note ID Note 1935468.1
- Oracle Support Bug 13704367 (PUBLIC HAS ALL PRIVILEGES ON SYS.DUAL), February 2012, https://support.oracle.com/epmos/faces/BugDisplay?id=13704367 (Note: Oracle has removed access to this bug)
- Why Public User Having All Privileges On sys.Dual Table, Last Updated 13 July 2011, My Oracle Support Note ID 418055.1
- January 2015 Critical Patch Update: Additional Information About Vulnerability CVE-2015-0393, January 24, 2015, My Oracle Support Node ID 1964164.1

History

January 20, 2015 – Initial Internal Analysis
January 21, 2015 – Published
January 25, 2015 – Updated to include information on applying database patch 19393542

About Integrigy

Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. AppDefend, our enterprise web application firewall is specifically designed for the Oracle E-Business Suite. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60602 USA
888/542-4802
www.integrigy.com

If you have any questions, comments or suggestions regarding this document, please send them via e-mail to info@integrigy.com.

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise.

Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice.

Integrigy's Vulnerability Disclosure Policy – Integrigy adheres to a strict disclosure policy for security vulnerabilities in order to protect our clients. We do not release detailed information regarding individual vulnerabilities and only provide information regarding vulnerabilities that are publicly available or readily discernible. We do not publish or distribute any type of exploit code. We provide verification or testing instructions for specific vulnerabilities only if the instructions do not disclose the exact vulnerability or if the information is publicly available.

Integrigy, AppSentry, and AppDefend are trademarks of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.