

Analysis of the October 2006 Critical Patch Update for the Oracle RDBMS

David Litchfield [davidl@ngssoftware.com]
17th October 2006



An NGSSoftware Insight Security Research (NISR) Publication
©2006 Next Generation Security Software Ltd
<http://www.ngssoftware.com>

Introduction

On the 17th of October 2006, Oracle released a Critical Patch Update (C.P.U.) – the 8th since they introduced their quarterly release cycle.

[<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2006.html>]

After a successful July 2006 C.P.U. release, where Oracle had all the patches ready, it's disappointing to see that Oracle have slipped back into their old, bad habits: at the time of the C.P.U. release patches were not available for the following platforms:

Version	Platform	Due
9.2.0.6	All Operating Systems	End of October
10.1.0.5	All Operating Systems	End of October
10.2.0.1	Linux (Power)	End of October
10.2.0.2	Windows	End of October

Analysis of Database Flaws

The following table details the flaws that have been fixed in this C.P.U. and describes the vulnerable component. These details will help DBAs perform a risk assessment of their systems. NGSSquirrel for Oracle [<http://www.ngssoftware.com/products/database-security/>] has also been updated to identify these exposure points.

ID	Schema	Package	Notes
DB01	XDB	DBMS_XDBZ	SQL Injection in ENABLE_HIERARCHY. The flaw actually lies in the

			ENABLE_HIERARCHY_INTERNAL procedure of the DBMS_XDBZ0 package. As XDB is not in the exclusion list for Oracle Application Server this flaw could be exploited without a user ID and password via the PLSQL Gateway.
DB02	MDSYS	SDO_DROP_USER_BEFORE	SQL Injection in Trigger – into an anonymous PL/SQL block. The trigger fires when a user issues the DROP USER statement. As the trigger is set to fire “before”, it fires before the system checks to make sure the user has the DROP USER privilege and is thus exploitable by anyone.
DB03	MDSYS	MD2	Buffer overflow in RELATE function (calls MDIREL C function) SQL Injection in TESSELATE_FIXED and TESSELATE. As MDSYS is not in the exclusion list for Oracle Application Server this flaw could be exploited without a user ID and password via the PLSQL Gateway.
DB04	SYS	DBMS_CDC_IMPDP	SQL Injection in BUMP_SEQUENCE. Also IMPORT_CHANGE_SET and IMPORT_SUBSCRIBER now call DBMS_ASSERT.SIMPLE_SQL_NAME
DB05	SYS	DBMS_CDC_IPUBLISH	SQL Injection in CREATE_CHANGE_TABLE – fixed “changeSourceType” in ChangeTable.class SQL Injection in CHANGE_TABLE_TRIGGER – fixed “fire” in ChangeTableTrigger.class CDC_DROP_CTABLE_BEFORE trigger is also an attack vector.
DB06	SYS	DBMS_CDC_ISUBSCRIBE	SQL Injection in PREPARE_UNBOUNDED_VIEW – fixed checkSubscribe in ChangeView.class.
DB07	SYS	DBMS_CDC_ISUBSCRIBE	SQL Injection in CREATE_SUBSCRIPTION – fixed createSubscription in SubscriptionHandle.class and changeSetAdvEnabled in SubscriptionHandle.class

DB08	SYS	DBMS_CDC_ISUBSCRIBE	<p>2nd Order SQL Injection in EXTEND_WINDOW_LIST – fixed getChangeSetWindow in SubscriptionWindow.class</p> <p>This can be exploited by creating a SET_NAME with embedded SQL. This flaw is fully discussed in the Oracle Hacker's Handbook.</p>
DB09	SYS	Unknown	Unknown
DB10	SYS	DBMS_SQLTUNE	SQL Injection in DROP_SQLSET, DELETE_SQLSET and SELECT_SQLSET
DB11	MDSYS	SDO_GEOM	Length checking added to RELATE function – then calls MD2.RELATE (see DB03 and DB22). As MDSYS is not in the exclusion list for Oracle Application Server this flaw could be exploited without a user ID and password via the PLSQL Gateway.
DB12	MDSYS	SDO_GEOR_INT	SQL Injection in COMPRESSDATA – fixed Compress.class
DB13	MDSYS	SDO_LRS	Invalid use of DBMS_ASSERT.SIMPLE_SQL_NAME in CONVERT_TO_LRS_LAYER, CONVERT_TO_LRS_LAYER_3D, CONVERT_TO_STD_LAYER and CONVERT_TO_STD_LAYER_3D. See http://archive.cert.uni-stuttgart.de/archive/bugtraq/2006/07/msg00489.html
DB14	XDB	XDB_PITRIG_PKG	SQL Injection in PITRIG_DROP and PITRIG_DROPMETADATA. PITRIG_DROP is called from the XDB.XDB_PI_TRIG trigger.
DB15	XDB	DBMS_XDBZ	SQL Injection in DISABLE_HIERARCHY_INTERNAL
DB16	SYS	DBMS_CDC_ISUBSCRIBE	SQL Injection SUBSCRIBE – fixed validateViewName in Subscribe.class
DB17	MDSYS	SDO_DROP_USER	SQL Injection in trigger.
DB18	MDSYS	SDO_TUNE	Patches not available – but could be EXTENT_OF function which is vulnerable to SQL injection

DB19	SYS	DBMS_SCHEDULER	Patch not available – possible buffer overflow based upon scoring
DB20	MDSYS	SDO_3GL	Buffer overflow in GEOM_OPERATION
DB21	MDSYS	SDO_CS	SQL Injection and buffer overflow in TRANSFORM_LAYER
DB22	MDSYS	SDO_GEOM	See DB11

---0000000---