Which database is more secure?
Oracle vs. Microsoft

David Litchfield [davidl@ngssoftware.com]
21st November 2006

An NGSSoftware Insight Security Research (NISR) Publication

http://www.ngssoftware.com

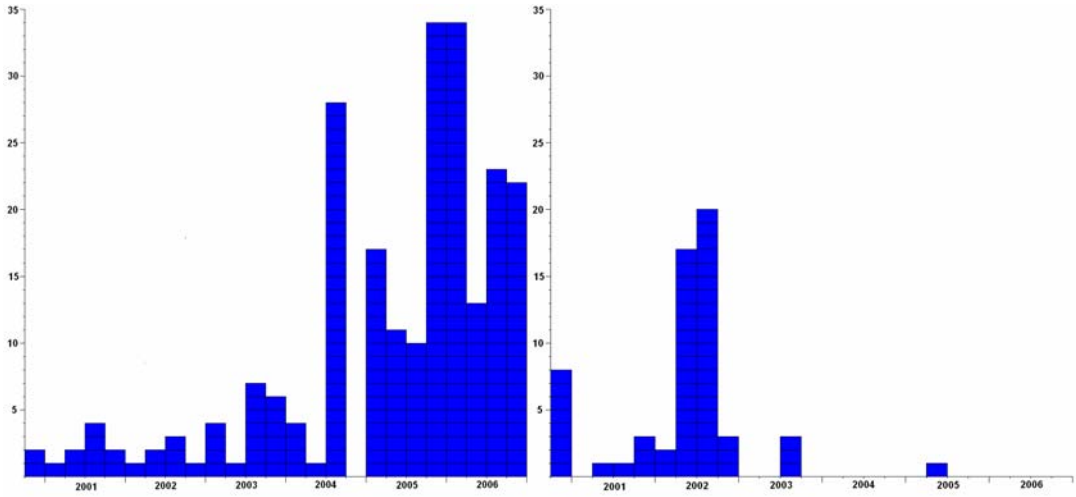
Introduction

This paper will examine the differences between the security posture of Microsoft's SQL Server and Oracle's RDBMS based upon flaws reported by external security researchers and since fixed by the vendor in question. Only flaws affecting the database server software itself have been considered in compiling this data so issues that affect, for example, Oracle Application Server have not been included. The sources of information used whilst compiling the data that forms the basis of this document include:

The Microsoft Security Bulletins web page
The Oracle Security Alerts web page
The CVE website at Mitre.
The SecurityFocus.com website

A general comparison is made covering Oracle 8, 9 and 10 against SQL Server 7, 2000 and 2005. The vendors' flagship database servers are then compared.

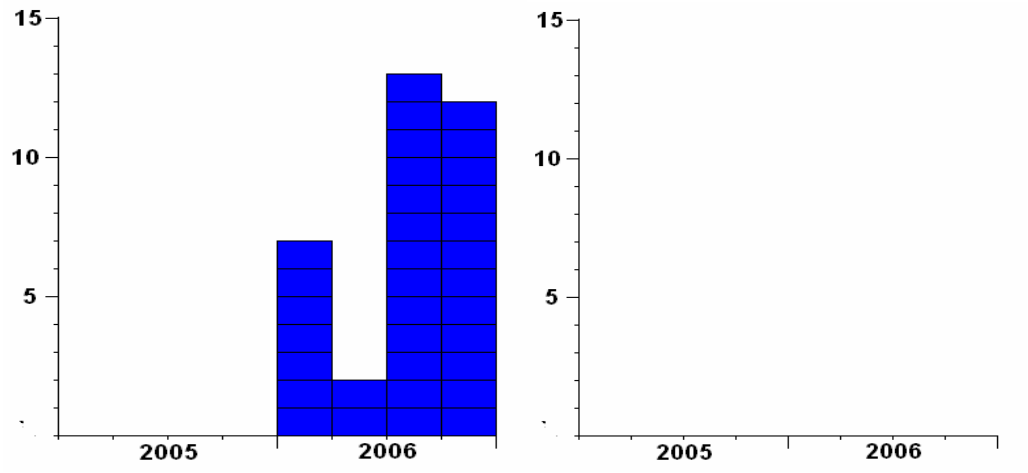
The Comparison



Oracle **Microsoft**

[See below for larger graphs]

The two graphs above show the number of security flaws in the Oracle and Microsoft database servers that have been discovered and fixed since December 2000 until November 2006. Each block represents a single issue with the sole exception of the single block in Q2 2005 of the Microsoft graph. This represents Service Pack 4 and whilst there are no related security bulletins or bugs listed on bugtraq the author felt it worthy of inclusion.



Oracle 10g Release 2 **Microsoft SQL Server 2005**

These two graphs indicate flaws that have been discovered by external security researchers in both vendors' flagship database products – namely Oracle 10g Release 2 and SQL Server 2005. No security flaws have been announced for SQL Server 2005.

It is immediately apparent from these four graphs that Microsoft SQL Server has a stronger security posture than the Oracle RDBMS.

Interpretation of results - some Q and A

Do Oracle's results look so bad because it runs on multiple platforms?
No – pretty much most of the issues are cross-platform. In the 10gR2 graph every flaw affects every platform.

Do the SQL Server 2005 results have no flaws because no-one is looking at it?
No – I know of a number of good researchers are looking at it – SQL Server code is just more secure than Oracle code.

Do you have any predictions on the Oracle January 2007 Critical Patch Update?
Maybe – NGSSoftware are currently waiting for Oracle to fix 49 security flaws – these will be fixed sometime in 2007 and 2008.

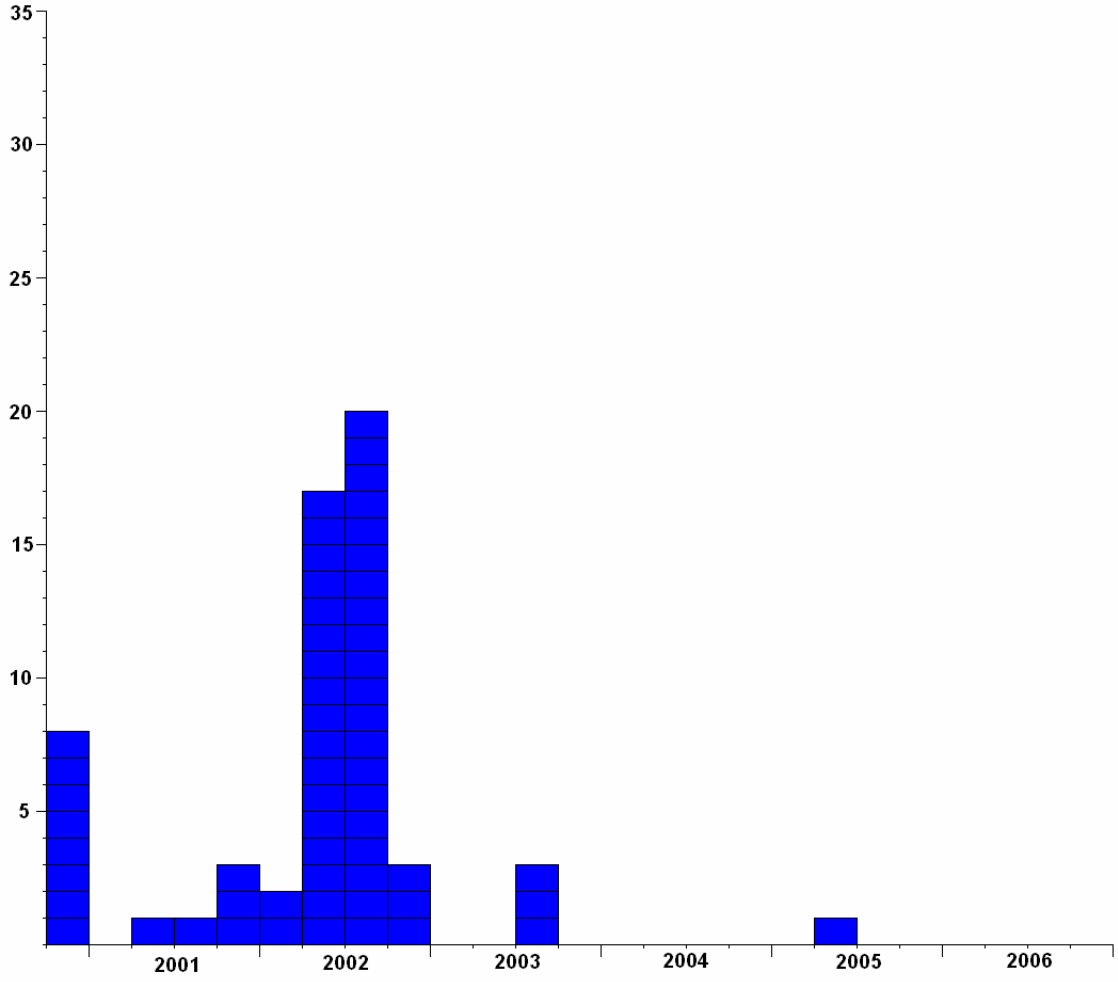
Do these results contain unfixed flaws?
No – only those that have been publicly reported and fixed are in the data.

Why have there been so little bugs found in SQL Server since 2002?
Three words: Security Development Lifecycle – SDL. SDL is far and above the most important factor. A key benefit of employing SDL means that knowledge learnt after finding and fixing screw ups is not lost; instead it is ploughed back into to the cycle. This means rather than remaking the same mistakes elsewhere you can guarantee that new code, whilst not necessarily completely secure, is at least more secure than the old code.

Does Oracle have an equivalent of SDL?
Looking at the results, I don't think so. Added to this that Oracle keep making the same basic mistakes and that some of their security "fixes" indicate that they don't understand the problems they're trying to fix. See http://seclists.org/bugtraq/2005/Oct/0056.html for more information.

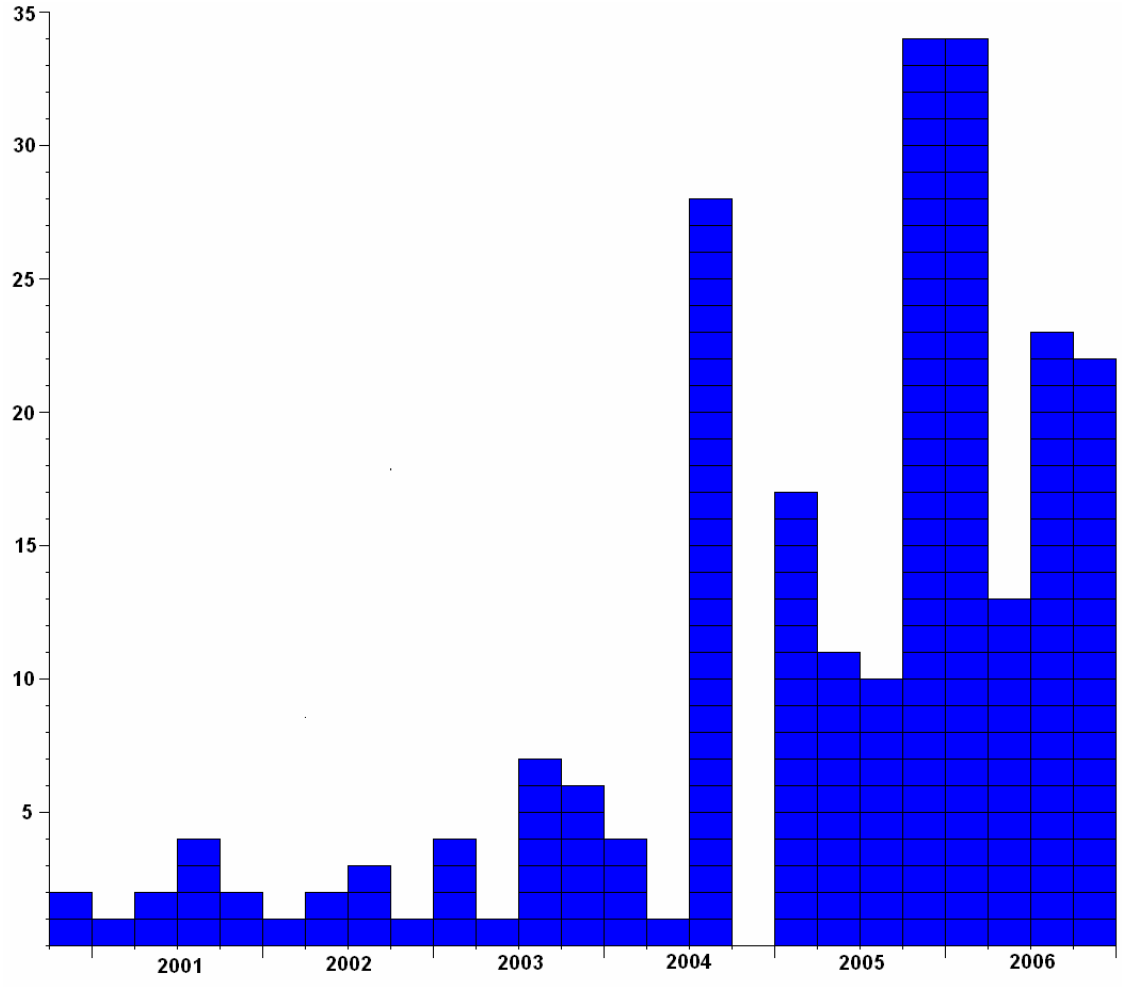
Microsoft SQL Server

Security issues and fixes in SQL Server 7, 2000 and 2005 since December 2000 to November 2006. Five MDAC security flaws over this period of time have not been included in these results because MDAC is part of Windows and *not* SQL Server.



Oracle

Security issues and fixes in Oracle 8, 9 and 10 since December 2000 to November 2006. Only security issues found in the TNS Listener and the RDBMS itself have been included in the following graph. This means issues found in components such as the Intelligent Agent or the Oracle Application Server have *not* been included.



Conclusions
Despite what the numbers clearly show these results will be contested by many; it is hoped that, since the author is responsible for finding many of these issues and thus speaks with some authority on such matters, there won't be too many though.

The conclusion is clear – if security robustness and a high degree of assurance are concerns when looking to purchase database server software – given these results one should not be looking at Oracle as a serious contender.

Appendix A – Microsoft SQL Server Flaws

October – December 2000

xp_displayparamstmt overflow	CAN-2000-1081	MS00-092
xp_enumresultset overflow	CAN-2000-1082	MS00-092
xp_showcolv overflow	CAN-2000-1083	MS00-092
xp_updatecolvbm overflow	CAN-2000-1084	MS00-092
xp_peekqueue overflow	CAN-2000-1085	MS00-092

xp_printstatements overflow	CAN-2000-1086	MS00-092
xp_proxiedmetadata overflow	CAN-2000-1087	MS00-092
xp_SetSQLSecurity overflow	CAN-2000-1088	MS00-092
April – June 2001		
Admin Cached Connection	CAN-2001-0344	MS01-032
July – September 2001		
RPC D.o.S.	CAN-2001-0509	MS01-041
October – December 2001		
raiserror format string	CAN-2001-0879	MS01-060
formatmessage format string	CAN-2001-0879	MS01-060
xp_sprintf buffer overflow	CAN-2001-0542	MS01-060
January – March 2002		
OpenDataSource buffer overflow	CAN-2002-0056	MS02-007
OpenRowSet buffer overflow	CAN-2002-0056	MS02-007
April – June 2002		
xp_proxiedmetadata overflow	CAN-2002-0154	MS02-020
xp_mergelineages overflow	CAN-2002-0154	MS02-020
xp_controlqueueservice overflow	CAN-2002-0154	MS02-020
xp_createprivatequeue overflow	CAN-2002-0154	MS02-020
xp_createqueue overflow	CAN-2002-0154	MS02-020
xp_decodequeuecmd overflow	CAN-2002-0154	MS02-020
xp_deleteprivatequeue overflow	CAN-2002-0154	MS02-020
xp_deletequeue overflow	CAN-2002-0154	MS02-020
xp_displayqueuemesgs overflow	CAN-2002-0154	MS02-020
xp_oledbinfo overflow	CAN-2002-0154	MS02-020
xp_readpkfromqueue overflow	CAN-2002-0154	MS02-020
xp_readpkfromvarbin overflow	CAN-2002-0154	MS02-020
xp_repl_encrypt overflow	CAN-2002-0154	MS02-020
xp_resetqueue overflow	CAN-2002-0154	MS02-020
xp_unpackcab overflow	CAN-2002-0154	MS02-020
SQLXML buffer overflow	CAN-2002-0186	MS02-030
SQLXML XSS	CAN-2002-0187	MS02-030
July – September 2002		
pwdencrypt buffer overflow	CAN-2002-0624	MS02-034
bulk insert overflow	CAN-2002-0641	MS02-034
SQL Agents priv upgrade	CAN-2002-0642	MS02-034
password in setup.iss	CAN-2002-0643	MS02-035
DBCC ADDEXTENDEDPROC	CAN-2002-0644	MS02-038
DBCC INDEXFRAG overflow	CAN-2002-0644	MS02-038
DBCC UPDATEUSAGE overflow	CAN-2002-0644	MS02-038

DBCC CHECKCONSTRAINTS	CAN-2002-0644	MS02-038
DBCC SHOWCONTIG overflow	CAN-2002-0644	MS02-038
DBCC CLEANTABLE overflow	CAN-2002-0644	MS02-038
Sp_MScopyscriptfile sql/cmd inj.	CAN-2002-0645	MS02-038
sp_MSsetalertinfo	CVE-2002-1981	--
sp_MSSetServerPropertiesn	CVE-2002-1981	--
Name Resolution Buffer Overflow	CAN-2002-0649	MS02-039
Name Resolution Heap Overflow	CAN-2002-0649	MS02-039
Name Resolution strtok DoS	CAN-2002-0649	MS02-039
Name Resolution 0x0A reply DoS	CAN-2002-0650	MS02-039
xp_execresultset p. upgrade	CAN-2002-0721	MS02-043
xp_printstatements p. upgrade	CAN-2002-0721	MS02-043
xp_displayparamstmt p. upgrade	CAN-2002-0721	MS02-043

October – December 2002

Hello Bug (Buffer Overflow)	CAN-2002-1123	MS02-056
DBCC SHOWTABLEAFFINITY	CAN-2002-1137	MS02-056
Webtasks priv. upgrade	CAN-2002-1145	MS02-061

July – September 2003

Named Pipe Priv. Upgrade	CAN-2003-0230	MS03-031
Named Pipe D.o.S.	CAN-2003-0231	MS03-031
LPC Buffer Overrun	CAN-2003-0232	MS03-031

April – June 2005

Service Pack 4	None	No advisories

Notes – what's not been included and why:
MDAC security flaws have not been included in these results because MDAC is part of Windows and *not* SQL Server. This covers the following bulletins:

MS02-040
MS02-065
MS03-033
MS04-003
MS06-014

One of the issues discussed in MS02-056 is a buffer overflow in the FoxPro ODBC driver and so is not included – see http://www.scan-associates.net/papers/foxpro.txt

Appendix B – Oracle RDBMS Security Flaws

October – December 2000

Listener Command	1	CVE-2000-0818	8.1.7
Oracle JVM	10	CVE-2001-0326	8.1.7

January – March 2001				
Redirect DoS	13	CVE-2001-0513	8.1.7	
April – June 2001				
Listener Overflow	15	CVE-2001-0498	8.1.7	
Listener DoS	16	CVE-2001-0498	8.1.7	
July – September 2001				
Offset_to_data heap overflow	14	CVE-2001-0515	8.x	
Requestor_Version DoS	14	CVE-2001-0516	8.x	
Max Data Size DoS	14	CVE-2001-0517	8.x	
Fragmentation attack	14	CVE-2001-0518	8.x	
October – December 2001				
Oracle Race Condition	20	CVE-2001-0832	8.x	9.0.1
Oracle Label Security	21	CVE-2001-0831	8.1.7	
January – March 2002				
Single Byte DoS	--	CVE-2002-0509		
Extproc Library Loading	29	CVE-2002-0567	9	
April – June 2002				
Left outer join sql	33	CVE-2002-0571	9	
SERVICE_NAME overflow	34	CVE-2002-0965	9	
July – September 2002				
Listener Debug DoS	38	CVE-2002-0856	9	8
Listener format string 1	40	CVE-2002-0857	9	8
Listener format string 2	40	CVE-2002-0857	9	8
October – December 2002				
SERVICE_CURLOAD DoS	42	CVE-2002-1118	9	8
January – March 2003				
BFILENAME Buffer Overflow	48	CVE-2003-0096	9	8
TZ_OFFSET Buffer Overflow	49	CVE-2003-0096	9	8
TO_TIMESTAMP_TZ Overflow	50	CVE-2003-0096	9	8
Long username overflow	51	CVE-2003-0095	9	8
April – June 2003				
CREATE DBLINK overflow	54	CVE-2003-0222	9	8
July – September 2003				
Extproc Overflow	57	CVE-2003-0634	9	

XDB HTTP long username overflow	58	CVE-2003-0727	9
XDB HTTP long password overflow	58	CVE-2003-0727	9
XDB FTP long username overflow	58	CVE-2003-0727	9
XDB FTP long password overflow	58	CVE-2003-0727	9
XDB FTP TEST overflow	58	CVE-2003-0727	9
XDB FTP UNLOCK overflow	58	CVE-2003-0727	9

October – December 2003

oracle long arg overflow	59	CVE-2003-0894	9
wwv_form.genpopuplist SQL Inj.	61	CVE-2003-1193	9
wwv_ui_lovf.show SQL Inj.	61	CVE-2003-1193	9
ORG_CHART.SHOW SQL Inj.	61	CVE-2003-1193	9
wwa_app_module.link SQL Inj.	61	CVE-2003-1193	9
wwv_dynxml_generator.show	61	CVE-2003-1193	9

January – March 2004

FROM_TZ Buffer Overflow	64	CVE-2003-1208	9
TIME_ZONE Buffer Overflow	64	CVE-2003-1208	9
NUMTODSINTERVAL Overflow	64	CVE-2003-1208	9
NUMTOYMINTERVAL Overflow	64	CVE-2003-1208	9

April – June 2004

SOAP DoS	65	--

July – September 2004

28 Issues in Alert 68	68

January – March 2005
17 Issues in Jan2005CPU
April – June 2005
11 Issues in Apr2005CPU
July – September 2005
10 Issues in Jul2005CPU
October – December 2005
29 Issues in Oct2005CPU
January – March 2006
29 Issues in Jan2006CPU
April – June 2006
13 Issues in Apr2006CPU
July – September 2006
23 Issues in Jul2006CPU
October – December 2006
22 Issues in Oct2006CPU

The following affects Oracle 10g Release 2:
Jan2006CPU DB09, DB12, DB13, DB17, DB18, DB25, DB27

Apr2006CPU DB05, DB08
Jul2006CPU DB06, DB08, DB09, DB10, DB11, DB12, DB13, DB14, DB16, DB17, DB18, DB19, DB20
Oct2006CPU DB02, DB04, DB05, DB06, DB07, DB08, DB09, DB12, DB13, DB14, DB15, DB17