

# The Oracle Security Patch: The First of Many

by Paul C Zikopoulos and Chris Eaton

**\*\* Images are linked to actual Web sites where possible \*\***

Oracle recently shipped its first [installment](#) of its [quarterly security patching cycle](#). This security patch affects most of Oracle's products, including Oracle 10gR1, Oracle 9iR1/R2, Oracle 8i, and the rest of their software portfolio.

Yes, you read that right: While some software companies have planned shipments for minor bug fixes and new feature delivery mechanisms, Oracle has had so many security fixes that they've had to make implementing them easier. How do they do that? They've created a planned delivery mechanism by which database administrators (DBAs) can count on a roll-up patch for all the security issues that have plagued Oracle in the previous quarter. Of course, the fact that these security issues remain unresolved until the patch is delivered, and Oracle refuses to provide any information as to the severity of the security flaws before-hand, has many analysts (including Gartner) concerned:



By Susan B. Shor  
[www.CRMBuyer.com](http://www.CRMBuyer.com),  
Part of the ECT News Network  
11/19/04 3:27 PM PT

**SECURITY**

## Oracle Patch Schedule Could Aid Hackers

**Gartner analysts Neil MacDonald and Rich Mogull wrote an advisory to clients last week stating that Oracle's refusal to release specific information about security vulnerabilities dealt with in a released patch increased risk for Oracle's customers.**

This first patch consists of 23 different security flaws: this for the [unbreakable Linux](#) database that Larry and the gang still talk about. Included in this security patch are fixes to some pretty significant problems that allow low level users to gain DBA privileges, including:

- SQL/PL injection attacks
- Access to directory objects
- **Buffer overflow vulnerabilities**
- and more...

Note the following commentary and keep in mind that one of the security issues that this patch solves is a **buffer overflow** problem:

**Breakable**

**'When they say  
their software is  
unbreakable,  
they're lying.'** -- Bruce Schneier

"If to them 'unbreakable' doesn't even mean they eliminate buffer overflows, how can it possibly mean they've secured the hard stuff?," says Bruce Schneier, founder and CTO of Counterpane Internet Security. "Fixing buffer overflows is the price of admission."

The problem is that this statement was made when the Oracle Unbreakable campaign was first released back in 2002! Now some 3 years later you could literally use the same quote. That doesn't sound too secure and unbreakable to us.

So what happens if a customer wants to patch their machines and protect themselves from these types of security exposures before Oracle's so called 'timely' patch? We're not sure really, and neither are customers. We do know that Oracle won't release details on what needs to be fixed between patches, so how would customers even know what to ask for if Oracle was to even provide it?

### ***So What About Security Certification Anyway?***

Oracle often attacks DB2 UDB on security claims, citing various certifications which thereby imply the database is more secure. At the most basic level, our customers should understand that no matter what security certification any vendor has obtained, 24 security flaws in your software stack in a single patch is a pretty serious issue.

So the first thing your customers should understand is that a certification doesn't mean your product is secure. In fact, the day Oracle launched its "[Unbreakable Campaign](#)" in 2002, Oracle was hit with a slew of security exposures (a number of them that Oracle *knew* about 3 months before the launch of this campaign - not very reassuring for customers).

Oracle will often cite various certifications for their product set. For example, the following was the backbone of a FUD campaign that claimed "Oracle has 17 certifications, DB2 UDB has 0...even SQL Server has 1".

## Competitive

Database Feature	Oracle	IBM DB2	MS SS2000
World Record Performance	✓	NO	NO
Unlimited scale up & scale out with RAC	✓	NO	NO
Sub-minute, transparent failover	✓	NO	NO
Successful Security evaluations	17	0	1
Self managing Database	✓	NO	NO
Multiple platform support	✓	Limited	Windows only

So what does the Oracle security effort really look like? As of December 04, 2004:

	Product	Release	Level	Criteria	Platform	Status
Custom Criteria	OLS 9i	9.2.0.1.0	EAL4	DBMS PP	Solaris 8, NT 4.0	Evaluated
	Oracle9i	9.2.0.1.0	EAL4	DBMS PP	Solaris 8, NT 4.0	Evaluated
	OLS 8i	8.1.7	EAL4	DBMS PP	Solaris 8	Evaluated
	Oracle8i	8.1.7	EAL4	DBMS PP	Solaris 8, NT 4.0	Evaluated
	Oracle8	8.0.5	EAL4	DBMS PP	NT 4.0	Evaluated
	Oracle7	7.2.2.4.13	EAL4	C.DBMS PP	NT 3.51	Evaluated
ITSEC	Oracle7	7.3.4.0.0	E3 / F-C2	E3/F-C2	NT 4.0	Evaluated
	Oracle7	7.2.2.4.13	E3 / F-C2	E3/F-C2	NT 3.51	Evaluated
	Oracle7	7.0.13.6	E3 / F-C2	E3/F-C2	Solaris 2.2	Evaluated
	Trusted Oracle7	7.2.3.0.4	E3 / F-B1	E3/F-B1	HP-UX CMW 10.16	Evaluated
	Trusted Oracle7	7.1.5.9.3	E3 / F-B1	E3/F-B1	Trusted Solaris 1.2	Evaluated
	Trusted Oracle7	7.0.13.6	E3 / F-B1	E3/F-B1	Solaris CMW 1.0	Evaluated
TCSEC	Oracle7	7.0.13.1	C2	C2	HP-UX BLS 8.0.4	Evaluated
	Trusted Oracle7	7.0.13.1	B1	B1	HP-UX BLS 8.0.4	Evaluated
Russian	Oracle8	8.0.3	IV	Russian Criteria	HP-UX 10.20	Evaluated
	Oracle7	7.3.4	III	Russian Criteria	NT 4.0	Evaluated
FIPS	Oracle9iAS	9.0.4	2	FIPS 140-2	Solaris 8	In Evaluation
	Oracle Advanced Security	8.1.6	2	FIPS 140-1	Solaris 2.6 SE	Evaluated

The previous figure shows a list of certifications that Oracle uses to try and portray the notion that it's a more secure database than DB2 UDB. First thing to note here is that of all these certifications, **0% are on Oracle 10g** and **89% are on products Oracle no longer actively sells or supports**. Furthermore, **not one certification is on Linux** (their strategic "unbreakable" platform), nor AIX. In fact, all of the certifications are on platforms that Oracle has, for the most part, openly noted as not being 'strategic' in their future direction. Finally, most of the products in the previous figure aren't even available for sale at the [Oracle Store](#) (when it's not [down](#) for maintenance).

It's important to note that security certifications simply verify that your product has the security features that you claim it has. It does not test for security holes in your product. Quite often, product security holes are found by independent groups like [Next Generation Security Software](#) (NGS), [Red Database Security](#), the [CERT Coordination Center](#), etc. to find and report on. In fact, people make a living by simply providing services, collateral, and survival guides on how to secure an Oracle database:

## Recently published Oracle Security Book by Pete Finnigan

**NEWS: SANS book updated to version 2.0** Pete Finnigan wrote a book for the SANS Institute ([www.sans.org](http://www.sans.org)) in their popular step-by-step series. The new guide published now is available from <http://store.sans.org> is called "Oracle Security Step By Step - A survival guide for Oracle security". The guide reached




Some even brag about how many security holes they've found as the cornerstone for their services and to prove to the world how well they understand security:

**Intelligent Solutions for  
an Evolving World**

**NGS** Software  
Next Generation Security Software Ltd

PRODUCTS




### NGSSquirrel for Oracle

You needn't be told that database security is important: whether it's financial accounts, client information, sales records or human resource details, whatever the data is, if it were to be stolen by a hacker or, perhaps even worse, by a competitor it would be disastrous. New database security vulnerabilities are being discovered all of the time and staying ahead of the attacker to protect your vital assets can be difficult to manage or achieve.

[A Helping Hand from the Oracle security experts](#)

No-one knows more about Oracle security than NGSSoftware. This isn't just sales talk; all one needs to do is look at Oracle's own security alerts to see how much we have contributed towards Oracle security. **NGS Research has found and helped to fix more Oracle vulnerabilities than anyone else.**



Who works for NGS? David Litchfield – a renowned security expert well known for discovering the Microsoft [SQL SLAMMER](#) virus that hit last year *and* the original flaws that broke the unbreakable database the day it was announced! His comments on Oracle are very interesting:



## Small security firm puts spotlight on big vendor bugs

Research company says it has discovered 67 undisclosed vulnerabilities in major vendors' software

"In general, bugs are getting harder to find but in some people's software you don't have to look very hard to find bugs, they just fall apart in your hands ... like Oracle's," Litchfield said in an interview Thursday.

What does all this mean? Is DB2 UDB invincible? No software is. However in the same fashion that Windows is subject to a host of security flaws and Linux is not, it would seem that the Oracle stack is subject to its fair share of security flaws that we're not seeing in the DB2 UDB space.

In fact, just like Microsoft, Oracle has to deal with such a large supply of security patches that it necessitates a coordinated and communicated delivery schedule (just like Microsoft Windows) for security patching alone! Clearly, this would suggest that there are more security exposures in Oracle than DB2.

Part of Oracle's new delivery mechanism include a directional grid which details which fixes are extremely important (in that they are easily exploitable) and which are not. Are they suggesting that customers pick and choose the security features to fix?

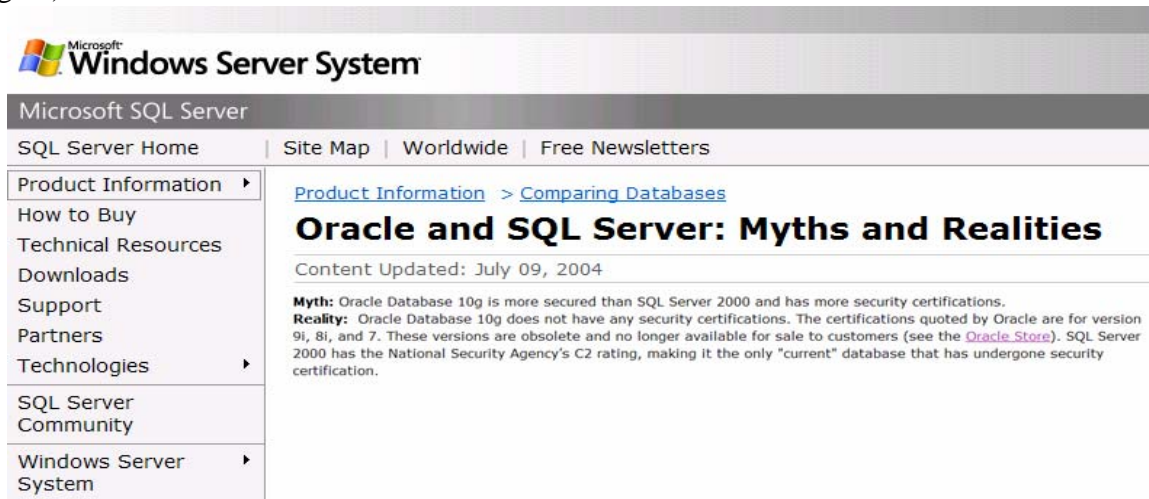
				RISK								
				Confidentiality		Integrity		Availability				
Vuln#	Component	Access Required (Protocol)	Authorization Needed (Package or Privilege Required)	Ease	Impact	Ease	Impact	Ease	Impact	Earliest Supported Release Affected	Last Affected Patch set (per Supported Release)	Work-around
DB01	Networking	SQL(Oracle Net)	Database (create database link)	Difficult	Wide	Difficult	Wide	Easy	Wide	8	8.0.6.3(8), 8.1.7.4(8), 9.0.1.4(9)	---
DB02	LOB Access	SQL(Oracle Net)	Database (read on database directory object)	Easy	Wide	---	---	---	---	8i	8.1.7.4(8), 9.0.1.5(9)	---
DB03	Spatial	SQL(Oracle Net)	Database (execute on mdsys.md2)	Difficult	Wide	Difficult	Wide	Easy	Wide	8i	8.1.7.4(8), 9.0.1.5(9), 9.2.0.5(9R2), 10.1.0.3.1(10g)	---
DB04	UTL_FILE	SQL(Oracle Net)	Database (read on database directory object)	---	---	Easy	Limited	---	---	9R2	9.2.0.5(9R2)	---
DB05	Diagnostic	SQL(Oracle Net)	Database	Difficult	Wide	Difficult	Wide	Easy	Wide	8i	8.1.7.4(8), 9.0.1.5(9), 9.2.0.4(9R2)	---
DB06	XDB	SQL(Oracle Net)	Database (execute on xdb.dbms_xdb)	Difficult	Limited	Difficult	Limited	---	---	10g	10.1.0.3.1(10g)	---
DB07	XDB	SQL(Oracle Net)	Database (execute on xdb.dbms_xdbzo)	Difficult	Limited	Difficult	Limited	---	---	9R2	9.2.0.5(9R2), 10.1.0.3.1(10g)	---
DB08	XDB	SQL(Oracle Net)	Database (execute on xdb.dbms_xdbzo)	Difficult	Limited	Difficult	Limited	---	---	10g	10.1.0.3.1(10g)	---
DB09	Dataguard	SQL(Oracle Net)	Database (execute on extfsys.dbms_extfil)	Difficult	Limited	Difficult	Limited	---	---	10g	10.1.0.3.1(10g)	---
DB10	Log Miner	SQL(Oracle Net)	Database (execute on dbms_logmnr)	Difficult	Limited	Difficult	Limited	---	---	9R2	9.2.0.5(9R2)	---
DB11	OLAP	SQL(Oracle Net)	Database (execute on olap.sys)	Difficult	Limited	Difficult	Limited	---	---	9R2	9.2.0.5(9R2), 10.1.0.3.1(10g)	---
DB12	Data Mining	SQL(Oracle Net)	Database (execute on dmshs.dmp_sys)	Difficult	Limited	Difficult	Limited	---	---	10g	10.1.0.3.1(10g)	---
DB13	Advanced Queuing	SQL(Oracle Net)	Database (execute on dbms_transform_extimp)	Difficult	Wide	Difficult	Wide	---	---	10g	10.1.0.3.1(10g)	---
DB14	Change Data Capture	SQL(Oracle Net)	Database (execute on dbms_cdc_dputil)	Difficult	Wide	Difficult	Wide	---	---	10g	10.1.0.3.1(10g)	---
DB15	Change Data Capture	SQL(Oracle Net)	Database (execute on dbms_cdc_impdp)	Difficult	Wide	Difficult	Wide	---	---	10g	10.1.0.3.1(10g)	---
DB16	Database Core	SQL(Oracle Net)	Database	Easy	Wide	Easy	Wide	---	---	10g	10.1.0.3.1(10g)	---
DB17	OHS	Network (HTTP)	Database (execute on ows_opt_lock)	Difficult	Limited	Difficult	Limited	---	---	8i	8.1.7.4(8), 9.0.1.5(9), 9.2.0.6(9R2)	---



So, now that you understand that security certifications and the security of your database aren't the same thing, and that history will show that Oracle has far more security exposures than DB2 UDB, what's the deal with certifications that count?

Software vendors that are vying for U.S.-based government business need to be [Common Criteria](#) certified. How does DB2 UDB fare in meaningful security certifications? Very well indeed...

It is however interesting to see Microsoft attacking Oracle 10g with their C2 certification, claiming that Oracle's certifications are on older products that are out of date (and we agree).



The screenshot shows the Microsoft SQL Server website. The header includes the Microsoft logo and "Windows Server System". Below this is a navigation bar with "Microsoft SQL Server" and links for "SQL Server Home", "Site Map", "Worldwide", and "Free Newsletters". A left sidebar contains a menu with "Product Information", "How to Buy", "Technical Resources", "Downloads", "Support", "Partners", "Technologies", "SQL Server Community", and "Windows Server System". The main content area is titled "Oracle and SQL Server: Myths and Realities" and includes a "Content Updated: July 09, 2004" note. The text discusses security certifications, contrasting a "Myth" (that Oracle Database 10g is more secured than SQL Server 2000) with a "Reality" (that Oracle Database 10g does not have any security certifications, while SQL Server 2000 has a C2 rating).

Microsoft  
**Windows Server System**

Microsoft SQL Server

SQL Server Home | Site Map | Worldwide | Free Newsletters

Product Information ▸  
How to Buy  
Technical Resources  
Downloads  
Support  
Partners  
Technologies ▸  
SQL Server Community  
Windows Server System ▸

[Product Information](#) > [Comparing Databases](#)

## Oracle and SQL Server: Myths and Realities

Content Updated: July 09, 2004

**Myth:** Oracle Database 10g is more secured than SQL Server 2000 and has more security certifications.  
**Reality:** Oracle Database 10g does not have any security certifications. The certifications quoted by Oracle are for version 9i, 8i, and 7. These versions are obsolete and no longer available for sale to customers (see the [Oracle Store](#)). SQL Server 2000 has the National Security Agency's C2 rating, making it the only "current" database that has undergone security certification.

Of course Microsoft fails to mention anything about Common Criteria – and the fact that C2 is an 'out-of-date' certification in itself.

So what's the bottom line when it comes to real certifications (like Common Criteria) on current versions of each vendor's database product?

***DB2 UDB = 1. Oracle = 0. Even SQL Server is trying...***

Finally, remember that chart on the Oracle Web site? Reality would have it as such....

**ORACLE**

PARTNER NETWORK

Welcome Paul ( Sign Out | Account )

ORACLE.COM | OTN | BUY | DOWNLOAD | CONTACT US

## Competitive

Database Feature	Oracle	IBM DB2	MS SS2000
World Record Performance	✓ 2.7 times slower than DB2	NO #1	NO 4.1 times slower than DB2
Unlimited scale up & scale out with RAC	✓ 16 nodes...but you can't buy it on the Web	NO 1,000	NO Still no
Sub-minute, transparent failover	✓ With expensive RAC	NO Sub-15 second	NO Delayed...
Successful Security evaluations	✓ Old products, out of date certifications	0 EAL4+ CC	1 Out of date
Self managing Database	✓ And you'll pay extra for features behind DB2	NO The Benchmark	NO Delayed...
Multiple platform support	✓ pSeries Linux???	Limited If it's relevant, we're there	Windows only

By the way, mark April 12<sup>th</sup>, 2005 on your calendars for your customer – because all the work they have to do today to patch Oracle security holes, they're going to do again when the next patch comes out.