Urgent Field Safety Notice

Ref. No.	**GPS_2012_28.1** IVD Product: cobas® 8000 data manager, Oracle version 10.2.0.4.0 Issue: Oracle TNS Listener vulnerability
Identifier:	GC-0534201
Type of Action	**Field Safety Corrective Action**
Document Date:	**18-Oct-2012**

Detail on affected device and/or system:

Product Name	**Part Number** (spare part)	**Lot Number**	**Expiration**
cobas® 8000 data manager:		N/A	N/A
DM 1.02.02	06458351001		
DM 1.02.03 (non barcode & barcode mode)	06499210001		
DM 1.02.05	06651674001		

The Oracle Software is pre-installed on all cobas® 8000 data manager.

Summary of Issue	Oracle TNS Listener vulnerability. A vulnerability in Oracle's TNS-listener component allows attackers to modify the content of a database from a remote system.
Summary Action required	Roche Diagnostics offers mitigation paths for the affected Units, please refer to the section *"Actions to be Taken by the User"*
Contacts	Technical Services: Country:

Description of the Problem:

Oracle confirmed a critical vulnerability in their TNS-listener component by an insecure default configuration. The TNS Listener can be considered as an authentication and redirection component between the client and the database.
The root cause of the weakness is that Oracle allows unauthenticated remote registration of databases under certain circumstances. The issue might allow an attacker to modify data stored in the Roche product.

Risk Assessment:

Although the current probability of occurrence for an attack scenario is "remote", if the issue were to occur, the integrity and correctness of patient results could be affected. This would lead to serious health consequences. The detectability of an attack and subsequent manipulation of data is considered being "uncertain or late" to "not possible".

Actions to be taken by the User:

All mitigation actions – blocking of external connections to the TNS Listener - will be executed either via remote service or via a Roche Diagnostics representative within the next 3-4 months. In case of a service visit you will be contacted by your local customer support representative to schedule the completion of the mitigation actions.
No actions are required by the user.

To date no case of an attack abusing the vulnerability in the Oracle TNS-listener in Roche Diagnostics Systems is known and the potential threat is rated being "remote".

If you have any further questions, please contact your local customer support representative.