Oracle Security Alert 58
Dated: 18 August 2003
Severity: 1

Buffer Overflow in the XML Database of Oracle *9i* Database Server

Description

A set of potential buffer overflows has been discovered in the XML Database (XDB) functionality of the Oracle9*i* Database Release 2. A knowledgeable and malicious user can exploit these buffer overflows to cause a Denial of Service (DoS) attack against and/or capture an active user session of the Oracle9*i* Database Server.

Products Affected

- Oracle9*i* Database Release 2

Oracle9*i* Database Release 1 and earlier versions are **not** affected.

Platforms Affected

See Patch Availability Matrix below.

Required conditions for exploit

There is an authenticated database user (i.e., valid login required), **or** the FTP and HTTP servers are enabled in the XML Database.

Risk to exposure

Unless you connect the database directly to the Internet (e.g., no intervening application server or firewall), a remote buffer overflow attack via the Internet is, in Oracle's opinion, unlikely. These vulnerabilities are highly susceptible to an insider attack originated on the corporate Intranet if best practices for secure configuration of the Oracle database are not followed; i.e., you should apply the patch in a timely manner.

Oracle strongly recommends that you do not connect your database directly to the Internet.

How to minimize risk

There are no workarounds that fully address these potential security vulnerabilities. However, you can reduce the risk of exposure by disabling the FTP and HTTP servers in the XML Database.

(Note: Both services are installed and enabled *by default*, and cannot be enabled and disabled individually.)

Disable both the FTP and HTTP servers in the XML Database, as follows:

1. In the Oracle9*i* Database Server INIT.ORA configuration file, on the "dispatchers" parameter line, remove the substring value "(SERVICE=<sid-name>XDB)", where <sid-name> represents the SID of the database.

2. Restart the database.

Follow best practices for database, (http://otn.oracle.com/deploy/security/oracle9i/pdf/9ir2_checklist.pdf and http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf,) and for IT deployments of firewalls, etc.

Ramification for CUSTOMER
Customers are vulnerable unless the patch is applied.

Oracle strongly recommends that customers review the severity rating for this Alert and patch accordingly. For a definition of severity ratings see http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf.

Patch Information
The patch listed in the Patch Availability Matrix fixes the potential vulnerabilities identified above, and enhances the robustness of the XML Database functionality.

Fixed by
Oracle9*i* Database Release 2, version 9.2.0.3 patchset is a required upgrade for the XML Database. The patch specified in the Patch Availability Matrix is to be installed on top of the 9.2.0.3 patchset.

This fix is included in the Oracle9*i* Database Release 2, 9.2.0.4 patchset.

There are no plans to release patches for 9.0.1.x, 8.1.7.x, 8.1.6.x, 8.1.5.x, 8.0.5.x, 7.3.x, or other patchsets of the supported releases because these releases are **not** affected.

Download the patch from the Oracle Support Services web site, Metalink (http://metalink.oracle.com).

1. Click on the **Patches** button.
2. Click on the "**New** Metalink Patch Search".
   If you are not on the "Simple Search" screen, click on the "Simple" button to get to the "Simple Search" screen.
3. Refer to the Patch Availability Matrix below to determine the patch number required.
4. In the "Search By" option select "Patch Numbers" from the drop-down menu, and enter the required patch number in the box.
5. Click on the "Go" button.
6. Select the required platform and language.
7. Click on the "Download" button.
8. Recommended: you should also click on the "View README" button for additional information and instructions.

Please review Metalink, or check with Oracle Support Services periodically for patch availability if the patch for your platform is unavailable at this time.

Oracle strongly recommends that you backup and comprehensively test the stability of your system upon application of any patch prior to deleting any of the original file(s) that are replaced by the patch.

Patch Availability Matrix

Platforms	9.2.0.3
Sun Solaris (32-bit)	3058991
Sun Solaris (64-bit)	3058991
IBM AIX 4.3.3 and 5L (32-bit)	---
IBM AIX 4.3.3 (64-bit)	3058991
IBM AIX Based 5L(64-bit)	3058991
MS Windows NT/2000/XP	ECD: September 2003
HP-UX (32-bit)	---
HP-UX (64-bit)	3058991
HP Tru64	3058991
LINUX	3058991
LINUX 390	ECD: August 2003
LINUX IA64	---
INTEL SOLARIS	---
DATA GENERAL	---
UNIXWARE	---
IBM NUMA-Q	---
SGI-IRIX-64	---
Siemens-64	---
Novell	---
OpenVMS	3058991
IBM OS/390 (MVS)	3058991
NEC	---
HP IA64	ECD: August 2003

--- : The Oracle Database Release/Version is not available for this platform.
ECD: Expected Completion Date

Credits

Oracle Corporation credits David Litchfield, of Next Generation Security Software Ltd., for the discovery of a subset of the vulnerabilities addressed in this alert. The Next Generation Security Software Advisory is available at http://www.nextgenss.com/research/advisories.html

Modification History

18-AUG-03: Initial release, Version 1