Oracle Security Alert #57
Released: 23 July 2003
Updated: 4 September 2003
Severity: 1

Comprehensive fix for EXTPROC vulnerabilities

Description

This Security Alert update supersedes all previous versions of the separate Security Alerts #29 and #57, and addresses all known potential vulnerabilities in the EXTPROC facility of the Oracle Database Server.

The issues addressed are:

- Utilizing an Oracle Listener configured with a TCP protocol address, a knowledgeable and malicious user can write an exploit that connects to an Oracle Database server's EXTPROC OS process without having to provide a database username and password. As such, it is possible to make arbitrary calls to the underlying OS and potentially gain unauthorized administrative access to the machine hosting the Oracle Database server. The EXTPROC functionality is installed by default in the Oracle Database installation if the "Typical Installation" option is chosen from the Oracle Universal Installer menu. EXTPROC is used by Oracle's PL/SQL software to make calls to the operating system.
- A subsequent update to the fix for the issue described above, previously released as Security Alert 57.

  These potential vulnerabilities can be exploited in some cases without a username and password. Therefore, **Oracle strongly recommends that this patch be applied as soon as possible**.

  Products Affected

  - Oracle9*i* Database Release 2
  - Oracle9*i* Database Release 1
  - Oracle8*i* Database (8.1.x – all releases)

  Platforms Affected

  See Patch Availability Matrix.

  Required conditions for exploit

  Network access to the database server.

  Risk to exposure

  Risk to exposure is high, as a valid username and password is not needed in all cases to exploit this potential vulnerability.

  These vulnerabilities are susceptible to an insider attack originating on a corporate intranet, but Oracle believes that the likelihood of exploit is minimal if best practices for a database are followed. Unless you connect to the database directly from the Internet (e.g., no intervening application server or firewall), a remote buffer overflow attack via the Internet is, in Oracle's opinion, unlikely. Oracle strongly recommends that you do not connect your database directly to the Internet.

  How to minimize risk

A patch is available (see below). Apply the patch listed in the Patch Availability Matrix, or perform the steps required listed in the **Workaround** section. Follow Oracle's best practices for the database by consulting http://otn.oracle.com/deploy/security/oracle9i/pdf/9ir2_checklist.pdf and http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf, and consider deployment of firewalls, etc.

Workaround

Use the following workarounds for all releases previous to Oracle9i Database Server Release 9.2.0.2. Apply these workarounds on all releases of the Oracle Database Server if you do not intend to apply the available patch (see Patch Availability Matrix below).

If the PL/SQL EXTPROC functionality is **not** required, it is recommended that it be removed from the machine hosting the Oracle Database Server. Edit both $ORACLE_HOME/NETWORK/ADMIN/**TNSNAMES.ORA** and $ORACLE_HOME/NETWORK/ADMIN/**LISTENER.ORA** (located in a Unix directory structure and its equivalent directory in Windows) and remove one of the following entries from each of the configuration files, depending upon the OS and the release of the Oracle Database Server installed:

- icache_extproc
- PLSExtproc
- extproc

Also, delete the "extproc" executable from the machine hosting the Oracle Database Server.

If the PL/SQL EXTPROC functionality **is** required in your Oracle installation, there are 5 steps that must be taken in order to protect against the potential security vulnerability identified above.

1. Create two Oracle Net Listeners, one for the Oracle database and one for PL/SQL EXTPROC.

Do not specify any EXTPROC specific entries in the configuration files of the Oracle Listener for the database.

Configure the Oracle Listener for PL/SQL EXTPROC with an IPC protocol address only.

If TCP connectivity is required, configure a TCP protocol address, but use a port other than the one the Oracle Listener for the database is using. Ensure that the Oracle Listener created for PL/SQL EXTPROC runs as an unprivileged OS user (e.g., "nobody" on Unix). On Windows platforms, run the Oracle Net Listener process as an unprivileged user and not as the Windows LOCAL SYSTEM user. Give this user the OS privilege to "Logon as a service."

2. If you have configured the Oracle Listener for PL/SQL EXTPROC with a TCP protocol address, modify the EXTPROC specific entry in $ORACLE_HOME/NETWORK/ADMIN/**TNSNAMES.ORA** to reflect the correct port for the new Oracle Listener.

3. If you have configured the Listener for PL/SQL EXTPROC with a TCP protocol address, ensure that the connections to this Oracle Listener can only originate from the hosts that need access to EXTPROC by doing the following.

Use the Oracle Net Services feature called "valid node checking" to allow or deny access to Oracle server processes from network clients with specified IP addresses. Set the following parameters in $ORACLE_HOME/NETWORK/ADMIN**/SQLNET.ORA** ($ORACLE_HOME/NETWORK/ADMIN/**PROTOCOL.ORA** in Oracle8i and prior releases) to enable the valid node checking feature:

tcp.validnode_checking = YES
tcp.invited_nodes = {list of IP addresses}
tcp.excluded_nodes = {list of IP addresses}

The first parameter turns on the valid node checking feature. The latter two parameters respectively specify the IP addresses that are permitted to make network connections and those that are prohibited from making network connections to the Oracle server processes.

Restrict access to the Oracle Listener for PL/SQL EXTPROC only. A separate $ORACLE_HOME/NETWORK/ADMIN/SQLNET.ORA file is required for this Oracle Listener. You can store this file in any directory other than the one in which the database LISTENER.ORA and SQLNET.ORA files are located. Copy the LISTENER.ORA with the configuration of the Oracle Listener for PL/SQL EXTPROC into this other directory as well. Before starting the Oracle Listener for PL/SQL EXTPROC, set the TNS_ADMIN environment variable (or Windows Registry parameter) to specify the directory in which the new configuration files for PL/SQL EXTPROC are stored.

4. Ensure that the file permissions on separate $ORACLE_HOME/NETWORK/ADMIN/LISTENER.ORA are set at either 640 or 644.

5. Change the password for any privileged database account, or for an ordinary user given administrative privileges that grant the ability to add packages or libraries and access system privileges in the database (such as CREATE ANY LIBRARY), to a strong, meaningful password, different from the default that is provided during the initial installation of Oracle.

Lock and expire all other accounts that are not being used in the database. Read Section 2 of the "Oracle9i Security Checklist" available on OTN at http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf for details.

Ramification for customer

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

Patch Information

The patches listed in the Patch Availability Matrix fix the potential security vulnerabilities identified above, and enhance the robustness of EXTPROC. The patch is included in the Oracle9*i* Database Release 2, Version 9.2.0.4 patchset.

The patch READMEs contain the patch application instructions/configuration guide.

Fixed by

An interim (one-off) patch for these issues is available for these affected database versions:

- Oracle 9*i* Database Release 2, version 9.2.0.3
- Oracle 9*i* Database Release 2, version 9.2.0.2

  Currently, due to architectural constraints, there are no plans to release a patch for versions 9.0.1.4, 8.1.7.4, 8.1.6.x, 8.1.5.x, 8.0.6.3, 8.0.5.x, 7.3.x, or other patchsets of the supported releases.

Download this one-off 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.

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

Special Notes:

- Customers running supported database releases previous to Oracle9*i* Database Release 9.2.0.2 must continue to use the above **Workaround**.
- Oracle recommends that **E-Business Suite 11*i*** customers apply the patches listed below.

Platforms	9.2.0.3	9.2.0.2
Sun Solaris (32-bit)	2988114	2988086
Sun Solaris (64-bit)	2988114	2988086
IBM AIX 4.3.3 and 5L (32-bit)	---	---
IBM AIX 4.3.3 (64-bit)	2988114	2988086
IBM AIX Based 5L(64-bit)	2988114	2988086
MS Windows NT/2000/XP	2973634	3056404
HP-UX 11.0 (32-bit)	---	---
HP-UX (64-bit)	2988114	2988086
HP Tru64	2988114	2988086
LINUX	2988114	2988086
LINUX 390	2988114	2988086
LINUX IA64	---	2988086
INTEL SOLARIS	---	---

DATA GENERAL	---	---
UNIXWARE	---	---
IBM NUMA-Q	---	---
SGI-IRIX-64	---	---
Siemens-64	---	---
Novell	---	---
Alpha OpenVMS	2988114	2988086
IBM OS/390 (MVS)	2990322	2990370
NEC	---	---
HP IA64	2988114	2988086

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

Credits

Oracle Corporation thanks Chris Anley, Mark Litchfield and David Litchfield of Next Generation Security Software Ltd., for discovering and researching these potential security vulnerabilities. The Next Generation Security Software Advisory is available at http://www.nextgenss.com/research/advisories.html.

Modification History

23-JUL-03: Initial release, Version 1
07-AUG-03: Removed unclear references to Alert 29, Version 2
04-SEP-03: Combined alerts 29 and 57, Version 3