THIS ALERT IS OBSOLETE AND SUPERSEDED BY ALERT 57

Oracle Security Alert 29
Dated: 06 Feburary 2002
Updated: 04 September 2003

~~Oracle PL/SQL EXTPROC in Oracle9i Database~~
~~Description~~
~~There is a potential security vulnerability in the Oracle PL/SQL package for External Procedures (EXTPROC) in Oracle9i Database.~~

~~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 package to make calls to the operating system. 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 authenticate himself. As such, he will be able to make arbitrary calls to the underlying OS and potentially gain unauthorized administrative access to the machine hosting the Oracle Database server.~~

~~Products affected~~
~~Oracle Database (Oracle9i, Oracle8i, Oracle8)~~

~~Platforms affected~~
~~All (Unix, Linux, Windows)~~

~~Workarounds~~
~~Use the following workarounds for 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** (located in a Unix directory structure and its equivalent directory in Windows) 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, or~~
~~* PLSExtproc, or~~
~~* 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 an 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 an Oracle Net 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 or denied 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 an ordinary user given administrative privileges in the database that has 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.~~

~~Patch Availability Matrix~~

~~Special Notes:~~

- ~~Customers running supported database releases up to and including Oracle9*i* Release 9.0.1.4 must continue to use the workaround identified above. Customers running Oracle9i Release 2 (9.2.0.2 and above) can apply the patch identified in the matrix below.~~

- ~~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 David Litchfield, of Next Generation Security Software Ltd., for discovering and promptly bringing this potential security vulnerability to Oracle's attention. The Next Generation Security Software Advisory is available at http://www.nextgenss.com/research/advisories.html.~~

~~**Modification History**~~

~~06-FEB-02: Initial release, Version 1~~
~~07-AUG-03: Updated with patch matrix, Version 2~~

04-SEP-03: Obsoleted Alert 29