

Database Security Brief
David Litchfield
18th November 2005

Q: I hear that local OS users can still launch external procedures in Oracle without going through the database. Should I really be worried about this?

A: If someone is "trusted" enough to be given local access then the chances are they won't pose a threat; but this isn't where the risk is coming from - it's the *remote* risk. That's right, *remote!* Before I explain why, let's briefly recap the whole problem with Oracle external procedures. From the beginning: PL/SQL procedures and functions can be extended by writing and hooking into C functions exported by dynamic link libraries or shared objects. Once the DLL is written the developer needs to tell Oracle about it and does so with a CREATE LIBRARY statement. They then wrap this in PL/SQL. When PL/SQL calls the C function the oracle process connects to the TNS Listener which then launches "extproc". Extproc loads the DLL and executes the function. At no stage is any of this authenticated. As such it is possible for an attacker to pretend to be Oracle and have extproc, via the Listener, load arbitrary libraries and execute arbitrary functions. Before a patch was produced for this an attacker could launch this attack remotely without a user ID and password. I explain this fully in "[Hackproofing Oracle Application Server](#)". Now, once the patch has been installed, only requests that originate from the local host will be honoured. [Oracle 8.1.7.4 is still vulnerable to remote attacks – Oracle refused to fix it for this version.] As such, if an attacker was local then they could still run commands as the Oracle user* but let's face it - if the user is local then 99 times out of 100 they're trusted. So should you be worried about this? Well as I said at the start of this answer - the risk still comes from *remote* attackers. How? By going through the database and UTL_TCP. By crafting special packets and sending them to the listener via UTL_TCP a remote database user can completely bypass any restrictions; they don't need the CREATE LIBRARY privilege - they just need access to UTL_TCP and, by default, PUBLIC has the execute permission on this package.

PL/SQL external procedures functionality has long been an Achilles Heel for Oracle. If you absolutely must have it, because your applications require it, then you'd do well to follow the risk mitigation steps detailed in [Oracle Security Alert 57](#). As an additional security recommendation, consider using a different service name other than the default PLSExtProc. Think about revoking public execute permissions on UTL_TCP as well.

* On a well configured server extproc should run as nobody.

References:

"Hackproofing Oracle Application Server".
<http://www.ngssoftware.com/papers/hpoas.pdf>.

Alert 57
<http://www.oracle.com/technology/deploy/security/pdf/2003alert57.pdf>