

[NEWS] Multiple Oracle Application Server SQL Injection Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0037.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/06/03

To: list@securiteam.com

Date: 6 Nov 2003 12:10:25 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Multiple Oracle Application Server SQL Injection Vulnerabilities

SUMMARY

Oracle's RDBMS, a leading database server package, supports stored packages and procedures using PL/SQL. These packages and procedures can be accessed through Oracle's Application Server's Portal module. Oracle Application Server is a web server designed for Oracle applications. Many of the PL/SQL packages and procedures are vulnerable to SQL Injection. Using these vulnerabilities, an unauthenticated attacker can gain access to all data in the database from the Internet.

DETAILS

By default, Oracle Application Server allows unauthenticated users on the web to access PL/SQL packages and procedures stored in the RDBMS. When a PL/SQL procedure is executed, it either does so with the security rights of the invoker or the definer. In the latter case, if a PL/SQL procedure defined by the powerful 'SYS' or 'SYSTEM' login is executed by a low privileged user that user can access data they would not directly be able to access. By executing such a procedure via Oracle Application Server and with these SQL Injection vulnerabilities, it is possible for an attacker to gain access to all data within the database. For example, an attacker

Securiteam: [NEWS] Multiple Oracle Application Server SQL Injection Vulnerabilities

could gain access to account details including database usernames and password hashes. Whilst there are some vulnerable packages that do allow this level of access, most do not. Those known to be vulnerable include the packages used for Portal DB Forms, Hierarchy, XML Components, and List of Values. All of the packages are required by the RDBMS so they cannot be deleted.

Fix Information:

NGSSoftware alerted Oracle to these vulnerabilities between September and October 2002, last year. Oracle has reviewed the code of the PL/SQL Packages and procedures and fixed these issues. A patch is available from Metalink. Please see

<http://otn.oracle.com/deploy/security/pdf/2003alert61.pdf>

<http://otn.oracle.com/deploy/security/pdf/2003alert61.pdf> for more details.

NGSSoftware advise Oracle database customers to review and install the patch as a matter of urgency.

ADDITIONAL INFORMATION

The information has been provided by <mailto:david@ngssoftware.com> David Litchfield.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.