

[NEWS] Oracle Workspace Manager SQL Injection Flaw

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-10/msg00037.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 23 Oct 2007 17:06:39 +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>

Oracle Workspace Manager SQL Injection Flaw

SUMMARY

The Workspace Manager in Oracle 10g release 1 and 2 and Oracle 9i is vulnerable to SQL injection.

DETAILS

Vulnerable Systems:

- * Oracle version 9i
- * Oracle version 10g release 1 and 2

The Workspace Manager, owned by SYS, contains a package called LT. This package is owned and defined by the SYS user and can be executed by PUBLIC. LT contains a procedure called FINDRICSET which calls the FINDRICSET package in the LTRIC package. This is vulnerable to SQL injection and can be abused by an attacker to gain SYS privileges.

Vendor Status:

Oracle was alerted to this flaw on the 22nd of August 2006. A patch has now been made available:

[NEWS] Oracle Workspace Manager SQL Injection Flaw

<<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html>>
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:davidl@xxxxxxxxxxxxxxxx>>
David Litchfield.
The original article can be found at:

<<http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-oracle-workspace-manager/>>
<http://www.ngssoftware.com/advisories/high-risk-vulnerability-in-oracle-workspace-manager/>

=====

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@xxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.