

# [UNIX] Oracle File Overwrite Security Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0084.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 10/28/01

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Subject: [UNIX] Oracle File Overwrite Security Vulnerability

Message-Id: <20011028220051.8EE49138BF@mail.der-keiler.de>

Date: Sun, 28 Oct 2001 23:00:51 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

## Oracle File Overwrite Security Vulnerability

---

### SUMMARY

There is a potential security vulnerability associated with the Oracle binary on several UNIX platforms. A non-privileged user (such as "nobody") invokes the oracle executable: as a result of the presence of the SETUID bit, the executable can be forced to write to a trace file in ORACLE\_HOME/rdbms/log directory and thereby overwrite existing log files or create new (unauthorized) files. The non-privileged user can also point the environment variable, ORACLE\_HOME, to an arbitrary directory in the operating system and thereby corrupt other files as well.

This article describes the workaround for this problem. For more information about this original problem, see our previous post:

< <http://www.securiteam.com/exploits/6I00P0K01G.html> > Linux Oracle security vulnerability (ORACLE\_HOME)

### DETAILS

Vulnerable systems:

All Oracle database server releases (8.0.x, 8.1.x, and 9.0.1)

## Securiteam: [UNIX] Oracle File Overwrite Security Vulnerability

### Workaround:

Change the file permissions on the oracle executable as follows:

```
% chmod o-x oracle
```

### Notes:

The workaround suggested above will permit only the owner of the oracle executable and users defined in the OS DBA group to run the oracle executable directly. With the execute permissions for "others" removed, other users cannot connect to an Oracle database server using the BEQ driver. If the BEQ driver is being used to connect to an Oracle database, a client program (such as SQLPLUS) will fork its processes and try to execute the oracle executable directly. This operation will fail because such a client program will run with the OS user's privileges that no longer have execution permission on the oracle executable. To avoid this problem, local users must connect to an Oracle database using the IPC driver that makes it possible to connect to a TNS listener listening on an Oracle database. The TNS listener will need to be started by a user that has execution permissions on the oracle executable.

### Patches:

The potential security vulnerability will be code-fixed in the next release of the Oracle database server that is Oracle9i, Release 2, only. All other releases of the Oracle database (8.0.x, 8.1.x, and 9.0.1) must use follow the workarounds specified above to circumvent the potential security vulnerability.

### ADDITIONAL INFORMATION

The information has been provided by <[mailto:secalert\\_us@oracle.com](mailto:secalert_us@oracle.com)>  
Oracle Security Alerts.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] Checkpoint VPN-1 SecuRemote Flaw (Username Verification)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)