

[UNIX] Oracle Trace Collection Security Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0081.html>

From: support@securiteam.com

Date: 10/28/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] Oracle Trace Collection Security Vulnerability

Message-Id: <20011028071434.BFCB8138BF@mail.der-keiler.de>

Date: Sun, 28 Oct 2001 08:14:34 +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 Trace Collection Security Vulnerability

SUMMARY

A potential security vulnerability has been discovered in Oracle's handling of the environment variable, ORACLE_HOME. A buffer overflow is caused when the Oracle binary, otrcrep, translates the environment variable, ORACLE_HOME, into a string of 240 or more bytes. The Oracle binary otrcrep runs with the SETUID oracle privileges in the operating system DBA group. The buffer overflow may be exploited by a local user to force overwriting of stack variables in shared memory including the return memory addresses and thereby execute arbitrary (or specific, malicious) code with the privileges of the oracle user and/or the DBA group privileges.

A patch and workaround are now available for this problem. For more information about the security hole, see our previous post:

<<http://www.securiteam.com/unixfocus/5AP082K55Y.html>> Local Security Vulnerability in 'dbsnmp' Binary (ORACLE_HOME)

DETAILS

Securiteam: [UNIX] Oracle Trace Collection Security Vulnerabili

Vulnerable systems:

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

Workaround:

If the ORACLE_HOME environment variable is being translated into a string of 240 or more bytes, disable Oracle Trace by setting its control parameter in init<SID>.ora as follows:

```
oracle_trace_enable=FALSE
```

Change the file permissions on all of the Oracle Trace executables as follows:

```
% chmod -s otrccol otrccref otrcfmt otrcrep  
% chmod 751 otrccol otrccref otrcfmt otrcrep
```

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>
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

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.

-
- **Previous message:** support@securiteam.com: "[EXPL] Remote DoS in 6tunnel"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)