CERT Advisory CA-2001-16 Oracle 8i contains buffer overflow in TNS listener

Original release date: July 03, 2001
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Oracle 8i

Overview

A vulnerability in Oracle 8i allows remote intruders to assume control of database servers running on victim machines. If the Oracle server is running on a Windows system, an intruder may also be able to gain control of the underlying operating system.

I. Description

The
COVERT labs at PGP Security have discovered a buffer overflow vulnerability in Oracle 8i that allows intruders to execute arbitrary code with the privileges of the TNS listener process. The vulnerability occurs in a section of code that is executed prior to authentication, so an intruder does not require a username or password.

For more information, see the COVERT Labs Security Advisory, available at

http://www.pgp.com/research/covert/advisories/050.asp

II. Impact

An intruder who exploits the vulnerability can remotely execute arbitrary code. On UNIX systems, this code runs as the 'oracle' user. If running on Windows systems, the intruder's code will run in the Local System security context.

In either case, the attacker can gain control of the database server on the victim machine. On Windows systems, the intruder can also gain administrative control of the operating system.

III. Solutions

Install a patch from Oracle. More information is available in Appendix A.

Appendix A

Oracle

Oracle has issued an alert for this vulnerability at

http://otn.oracle.com/deploy/security/pdf/nai_net8_bof.pdf

Oracle has fixed this potential security vulnerability in the Oracle9i database server. Oracle is in the process of backporting the fix to supported Oracle8i database server Releases 8.1.7 and 8.1.6 and Oracle8 Release 8.0.6 on all platforms. The Oracle bug number for the patch is 1489683.

Download the patch for your platform from Oracle's Worldwide Support web site, Metalink:

http://metalink.oracle.com Please check Metalink periodically for patch availability if the patch for your platform is not yet available.

Our thanks to COVERT Labs at PGP Security for the information contained in their advisory.

This document was written by Shawn V. Hernan. If you have feedback concerning this document, please send email to:

mailto:cert@cert.org?Subject=[VU#620495]%20Feedback%20CA-2001-16

Revision History

```
July 03, 2001: Initial Release
```