Oracle Security Alert #27
Reference date: 28 December 2001

Vulnerabilities in Oracle9*i* Application Server Web Cache

Products

Oracle9iAS Web Cache 2.0.0.x

Platforms affected

- MS Windows NT/2000 Server
- Sun SPARC Solaris
- HP-UX
- Linux
- Compaq Tru64 UNIX

Overview

1. **Bug 2114542**

   Old Unix installer program created incorrect file permissions on executable and configuration files allowing:

   - Arbitary local file overwrite of files accessible to "oracle" user.
   - Local privilege escalation to "oracle" user.
   - Local capture of the webcache admin account.

2. **Bug 2108464**

   Remote Denial-of-Service (DoS) vulnerability on ports 1100, 4000, 4001, and 4002.

3. **Bug 2107007**

   Remote DoS vulnerability in port 4000.

4. **Bug 2111358**

   Remote DoS vulnerability caused by buffer overflow in Windows 2000 and Windows NT.

Description of the problems

1. **Bug 2114542**

   It is possible for non-privileged user to start Oracle9iAS Web Cache by invoking $ORACLE_HOME/webcache/bin/webcached, which is a setuid oracle file. The user could specify environment variables and configuration files that would cause local files to be overwritten and commands to be run as the "oracle" user. The webcache Administrator password is stored in $ORACLE_HOME/webcache/webcache.xml. This file is readable by world and contains the password hash for the administrator account. By reading this file, a local user can attempt to crack the encryption.

2. **Bug 2108464**

   Sending multiple requests containing many null characters will cause a remote DoS.

3. **Bug 2107007**

   Requesting multiple periods will result in an access violation in the webcache daemon. It requires a manual restart (webcachectl start) to restart the admin service.

4. **Bug 2111358**

   An incorrectly checked buffer allowed remote DoS for a variety of long HTTP headers, header values, and GET requests. The initial symptom is that the daemon process will consume 100% of the CPU, but still serve pages. An remote attacker making multiple requests will eventually force resource starvation, hanging the daemon and requiring it to be manually killed, before restarting Oracle9iAS Web Cache.

Patch Solution

Oracle has fixed these potential security vulnerabilities in the 2.0.0.3 release of Oracle9iAS Web Cache.

Supported customers may download the release from Oracle's Worldwide Support web site, Metalink, http://metalink.oracle.com. Activate the "Patches" button to get to the patches web page. Enter patch number **2131605**, and activate the "Submit" button.

Alternatively, the release may be downloaded for evaluation on Windows NT, Solaris, hp, and Linux from Oracle Technology Network, http://otn.oracle.com/software/content.html

Credits

Oracle thanks the following for their assistance:

- George Hedfors of Defcom Security for reporting bug 2111358.
- Peter Gründl of KPMG, for reporting bugs 2108464 and 2107007.
- Mark Rowe of PenTest Limited, for reporting bug 2114542.